Anais do VII

Workshop de Pós-Graduação
Engenharia de Computação

22 de novembro

São Paulo
2018

Comissão Organizadora:

Composta por orientadores e alunos do Programa de Pós-Graduação de Engenharia Elétrica - área de Concentração em Engenharia de Computação, funcionários do PCS e um representante da Biblioteca da Engenharia Elétrica. Relacionados a seguir:

Profa. Dra. Solange Nice Alves de Souza, presidente
Prof. Dr. Pedro Luiz Pizzigatti Corrêa
Prof. Dr. Jorge Rady de Almeida Júnior
Profa. Dra. Anarosa Alves Franco Brandão
Dra. Ana Maria de Castro Badiali
Gabriel de Freitas Viscondi
Victor de Mendonça Carbonezi
Lesly Alejandra González Camacho
Michelet del Carpio
Mariza Ushijima Leone
Profa. Dra. Sandra Sayuri Sato

Comitê Científico:

O comitê Científico é composto por docentes, orientadores e pesquisadores colaboradores do Programa de Pós-Graduação em Engenharia Elétrica - área de Concentração em Engenharia de Computação. Relacionados a seguir:

Profa. Dra. Anarosa Alves Franco Brandão (USP)
Prof. Dr. Andre Riyuiti Hirakawa (USP)
Profa. Dra. Anna Helena Reali Costa (USP)
Prof. Dr. Carlos Eduardo Cugnasca (USP)
Profa. Dra. Cíntia Borges Margi (USP)
Dr. Cléber Gimenez Correa (UTFPR)
Prof. Dr. David Corrêa (UFABC)
Prof. Dr. Edison Spina (USP)
Prof. Dr. Edson Satoshi Gomi (USP)
Prof. Dr. Eduardo Raul Hruschka (USP)
Prof. Dr. Fábio Gagliardi Cozman (USP)
Prof. Dr. Fábio Levy Siqueira (USP)
Prof. Dr. Fabrício Rodrigues (UFMGS)
Profa. Dra. Fátima L. S. Nunes (USP)
Prof. Dr. Fernando Frota Redigolo (USP)
Prof. Dr. Flávio S. Correa da Silva (USP)
Prof. Dr. Glauber Bona (USP)
Profa. Dra. Graça Bressan (USP)
Prof. Dr. Hae Yong Kim (USP)
Prof. Dr. Jaime Simão Sichman (USP)
Dra. Janete Ribeiro (USP)
Prof. Dr. João Batista Camargo Jr (USP)
Prof.Dr. Jorge Kinoshita (USP)
Prof.Dr. Jorge Rady de Almeida Junior (USP)
Prof. Dr. João José Neto (USP)
Prof. Dr. Jorge Luis Risco Becerra (USP)
Prof. Dr. Kechi Hirama (USP)
Dr. Leandro Guarino (INPE)
Prof. Dr. Luiz Sergio de Souza (FATEC)
Profa. Dra. Liria Matsumoto Sato (USP)
Profa. Dra. Lúcia Filgueiras (USP)
Prof. Dr. Marcelo Morandini (USP)
Dra. Marcia Ito (IBM Research)
Prof. Dr. Marco Túlio Andrade (USP)
Prof. Dr. Marcos Antonio Simplicio Jr. (USP)
Dr. Nelson Tanomaru (USP)
Prof. Dr. Paulo Sérgio Cugnasca (USP)
Prof. Dr. Pedro Corrêa (USP)
Profa. Dra. Regina Silveira (USP)

Prof. Dr. Reginaldo Arakaki (USP)
Prof. Dr. Ricardo Nakamura (USP)
Prof. Dr. Ricardo L. A. Rocha (USP)
Profa. Dra. Selma S. S. Melnikoff (USP)
Prof. Dr. José Sidnei Colombo Martini (USP)
Profa. Dra. Solange N. Alves de Souza (USP)
Profa. Dra. Tereza C. M. Brito Carvalho (USP)
Prof. Dr. Wilson Vicente Ruggiero (USP)

Financiadores e Apoiadores:
O WPGEC 2018 foi financiado pelas seguintes empresas:

- Acesso Informática
- Accenture
- Everis

Apoio:

- Departamento de Engenharia de Computação e Sistemas Digitais
- Programa de Pós-Graduação de Engenharia Elétrica (PPGEE)

Organização:

- Programa de Pós-Graduação de Engenharia Elétrica da Escola Politécnica da USP (PPGEE/EPUSP) - Área de concentração: Engenharia de Computação
- Departamento de Engenharia de Computação da Escola Politécnica da USP (PCS/EPUSP).

Prêmios:
Serão selecionados trabalhos de qualidade destacada (mestrado, doutorado), dentre os trabalhos enviados para apresentação oral. Estes trabalhos serão selecionados pelo Comitê Científico do VII WPGEC. Os participantes também participarão da indicação dos melhores trabalhos dentre os apresentados apenas na forma de pôsteres.

Local do Evento:
O VII WPGEC realizado no Anfiteatro Prof. Paulo Ribeiro de Arruda e na sala C1-49 do Prédio de Engenharia Elétrica, localizado no seguinte endereço: Av. Prof. Luciano Gualberto, travessa 3, n°. 158, CEP.: 05508-010 - Cidade Universitária - São Paulo - SP.

São Paulo, 22 de novembro de 2018.
Comitê Organizador do VII WPGEC 2018

Catalogação na Publicação

Workshop de Pós-Graduação Engenharia de Computação

Anais do **VII** Workshop de Pós-Graduação em Engenharia de Computação – WPGEC, São Paulo, SP, 22 de novembro de 2018 / organizado por Solange N. A. Souza et al. – São Paulo: PCS/POLI/USP, 2018.

ISBN: 978-85-5338-002-2

1. Engenharia da computação. 2. Ciência da computação. 3. Ciência da informação. I. Universidade de São Paulo. Escola Politécnica. Programa de Pós-Graduação em Engenharia de Computação. II. T.

CDD 621.39

Elaborada pela Bibliotecária Ana Maria C. Badiali CRB-8/2368

Patrocínio

Apoio

Apresentação

VII Workshop de Pós-Graduação em Engenharia de Computação
São Paulo, 22 de novembro de 2018

O Workshop de Pós-Graduação de Engenharia de Computação 2018 – WPGEC 2018 – é um evento de ciência e tecnologia organizado pelo departamento de Engenharia de Computação e Sistemas Digitais (PCS) da Escola Politécnica da Universidade de São Paulo.
A Escola Politécnica da Universidade de São Paulo (EPUSP) oferece diversos programas de Pós-Graduação – mestrado, doutorado e doutorado direto. Dentre eles está o de Engenharia Elétrica, cuja Área de Concentração "Engenharia de Computação" é de responsabilidade dos professores do Departamento de Engenharia de Computação e Sistemas Digitais (PCS/EPUSP), sendo o curso reconhecido e avaliado regularmente pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes), fundação do Ministério da Educação (MEC), com nota "6" (entre 1 e 7). A área de concentração Engenharia de Computação do Programa de Pós-Graduação em Engenharia Elétrica (PPGEE) conta com três linhas de pesquisa relacionadas a seguir. **A) Sistemas de Informação e Aplicações Computacionais**, envolvendo sistemas computacionais e banco de dados com aplicações relacionadas ao agronegócio, gestão de dados científicos, qualidade de dados, ambiente, logística, governo, metro-ferroviários, aeronáuticos, confiabilidade, segurança crítica, automação, sistemas complexos e Big Data. **B) Organização de Sistemas Computacionais**, envolvendo redes de computadores; desempenho de sistemas Computacionais; segurança da informação e de redes; arquitetura de computadores; sistemas dedicados; arquitetura e processamento paralelos. **C) Metodologias de Computação** envolvendo inteligência artificial, sistemas multiagentes, visão computacional, ciência dos dados, robótica inteligente, aprendizado de máquina, técnicas adaptativas, engenharia de conhecimento, computação gráfica, realidade aumentada, interação humano-computador e computação na educação.

O Workshop de Pós-Graduação em Engenharia de Computação (WPGEC) tem por objetivo difundir as pesquisas e estimular a colaboração entre os alunos, pesquisadores e professores do PPGEE/EPUSP e a comunidade em geral. O local da sétima edição do WPGEC foi o prédio de Engenharia Elétrica da Escola Politécnica da Universidade de São Paulo, no dia 22/11/2018 (pcs.usp.br/wpgec). O WPGEC 2018 consistiu em sessões de apresentação de pôster de todos os trabalhos, apresentação oral de alguns destes e apresentações de keynotes speakers, relatando temas e demandas de pesquisa no Brasil relacionadas às áreas de Engenharia de Computação. Os resultados estão aqui publicados na forma de anais do WPGEC 2018. O WPGEC 2018 reuniu em torno de 150 participantes, que incluíram estudantes de pós-graduação da área de Engenharia de Computação, pesquisadores nacionais, técnicos e tomadores de decisão que atuam em instituições governamentais e privadas, e em empresas apoiadoras da pesquisa nacional.

São Paulo, 22 de novembro de 2018.
Comitê Organizador do VII WPGEC 2018

Agenda

Programação do WPGEC 2018

Horário	**Atividade**
8:00-9:00	Credenciamento
9:00-9:30	Sessão de Abertura
9:30-10:00	"Desafios da pesquisa em Engenharia da Computação para atender as demandas da sociedade brasileira" Prof. Dr. Eduardo Raul Hruschka, Escola Politécnica da USP
10:00-11:00	Coffee Break e Exibição de pôsteres
11:00-12:10	Apresentações de trabalhos selecionados
12:10-13:30	Recesso para Almoço
13:30-14:10	"Desafios da pesquisa em Engenharia da Computação na Saúde para atender as demandas da sociedade brasileira" Profa. Dra. Fátima L. S. Nunes, Escola de Artes, Ciências e Humanidades da USP
14:10-15:00	Apresentações de trabalhos selecionados
15:00-16:00	Coffee Break e Exibição de pôsteres
16:00-17:00	Sessão de premiação e encerramento

ARTIGOS DE MESTRADO

Combinando novidade e popularidade em recomendações personalizadas através do aprendizado do perfil do usuário

BERTANI, R. M.; COSTA, A. H. R.
Laboratório de Técnicas Inteligentes - EP/USP
e-mail: ricardo.bertani@usp.br; anna.reali@usp.br

***Abstract*—Recommender Systems have been an interesting tool to help users to find relevant content, once the amounts of on-line information vastly increase. A wide variety of algorithms have been proposed for this purpose, in particular those based on collaborative filtering, which often fail in sparse data, affecting the quality of recommendations. A hybrid algorithm based on diffusion has been proposed in the literature in order to mitigate this gap, however, it does not differentiate users according to their profiles. In this paper, a new diffusion-based algorithm is presented for learning user profiles and combining novel and popular items to make personalized recommendations. The experiments were performed in a high sparse dataset and show that the results outperforms those obtained by the original diffusion-based algorithm, in the same settings.**

***Keywords*— machine learning, recommender systems, sparsity data, diffusion-based algorithms.**

***Resumo*— Sistemas de recomendação têm sido uma interessante ferramenta no auxílio a usuários pela busca de conteúdo relevante, uma vez que a quantia de informações online aumenta consideravelmente. Uma ampla variedade de algoritmos foi proposta para esta finalidade; em particular aqueles baseados em filtragem colaborativa, que frequentemente falham em dados esparsos, afetando a qualidade das recomendações. Um algoritmo híbrido baseado em difusão foi proposto na literatura para mitigar essa lacuna, no entanto, este algoritmo não diferencia os usuários de acordo com seus perfis. Neste artigo, um novo algoritmo baseado em difusão é apresentado para aprender o perfil particular dos usuários e combinar itens populares e de novidade para a geração de recomendações personalizadas. Os experimentos foram conduzidos em um conjunto de dados altamente esparso e mostram que os resultados superam aqueles obtidos pelo algoritmo original baseado em difusão, sob as mesmas configurações.**

***Palavras-chave*— aprendizado de máquina, sistemas de recomendação, dados esparsos, algoritmos baseados em difusão**

***Classificação*— Mestrado**

***Categoria*— Qualificado**

I. Introdução

Sistemas de Recomendação (SR) são programas de computador capazes de realizar sugestões de conteúdo a usuários de acordo com a predição de suas preferências. Segundo [1], os conteúdos recomendados ao usuário, tais como músicas, livros, notícias, e até amigos em redes sociais podem ser representados pelo termo “item”. De acordo com [2], para que seja possível a realização de uma recomendação é necessário levar em consideração alguns conceitos fundamentais, tais como: algoritmos de filtragem, tipo de dados disponível e a medida de qualidade das recomendações. Na visão de [3], os algoritmos de filtragem podem ser classificados de acordo com seu tipo (baseados em conteúdo, colaborativos, baseados em conhecimento e híbridos) e de acordo com a abordagem adotada (baseado em memória ou baseado em modelo). Com relação ao tipo de dados disponível geralmente são explorados os atributos de usuários e itens, além das avaliações que os usuários atribuem a itens em um SR, as quais podem ser explícitas ou implícitas, sendo a primeira expressa através de um "*rating*"de um usuário para um item [4], e a segunda quando é necessário acessar dados de navegação do usuário (cliques em links, movimentos do mouse, download de conteúdo) para inferir suas preferências [5]. O principal tipo de algoritmo de filtragem, de acordo com a literatura, é o colaborativo, o qual sofre com dois problemas conhecidos: partida a frio (*cold-start*) e o problema dos dados esparsos (*sparsity data*) [6],[4].

O primeiro consiste na falta inicial de avaliações devido tanto a novos itens quanto a novos usuários; já o último ocorre devido ao alto número de itens e usuários no sistema acompanhados de uma quantia muito baixa de interações entre ambos, o que prejudica a identificação de uma vizinhança de usuários similares e afeta diretamente a qualidade das recomendações. Neste artigo é apresentado um novo algoritmo baseado em difusão, o qual é capaz de combinar itens populares e pouco conhecidos (novidade) nas recomendações de acordo com o perfil dos usuários, o que permite a geração de recomendações personalizadas. Resultados experimentais mostram que a nova abordagem supera o algoritmo baseado em difusão original e uma implementação básica do algoritmo colaborativo.

O artigo está organizado da seguinte forma. A seção II apresenta alguns trabalhos relevantes presentes na literatura dos SR. A seção III procura detalhar os algoritmos baseados em difusão, os quais suportam esta pesquisa. Na seção IV é apresentada a proposta desta pesquisa. Na sequencia, na seção V são descritos os experimentos e é realizada uma discussão dos resultados. Por fim na seção VI, são apresentadas as conclusões e os trabalhos futuros.

II. Trabalhos Relacionados

Diversas abordagens já foram consideradas na literatura dos SR: abordagens clássicas, como os algoritmos de filtragem baseados em conteúdo ou colaborativos; e abordagens mais modernas como os algoritmos baseados em difusão de massa

ou a aplicação de técnicas de aprendizado profundo [7], [6], [3], [8]. Entretanto, o algoritmo de filtragem colaborativa (FC) ainda é considerado o mais popular. Tal algoritmo explora informações prévias de um grupo de usuários similares para predizer o nível de interesse de um usuário por um item [9], e pode ser classificado como baseado em memória ou baseado em modelo, de acordo com [10] e [4]. No primeiro, todas informações de usuários e itens devem estar disponíveis em memória a todo momento, enquanto que no segundo gera-se um modelo probabilístico a partir dos dados, capaz de predizer o nível de interesse do usuário [1].

Os algoritmos FC baseados em memória também são conhecido na literatura como algoritmos "baseados em vizinhança"(*neighborhood-based*) [9], isto porque nesta abordagem busca-se encontrar uma vizinhança de usuários similares ao usuário alvo da recomendação para inferir suas preferências. Para a determinação da vizinhança de usuários são utilizadas algumas medidas de similaridade que consideram os *ratings* atribuídos aos itens, sendo a mais comum o coeficiente de correlação de Pearson [11], que mede o grau de correlação entre dois usuários, baseado na avaliação de ambos para o mesmo conjunto de itens.

Como tais medidas exploram os *ratings* presentes nos datasets, e estes são frequentemente bastante esparsos, tem-se que as vizinhanças necessárias para o cálculo são insuficientes e portanto afetam as recomendações, o que é conhecido como "problema dos dados esparsos" [12]. Algumas soluções conhecidas exploram alternativas como *tagging social* [13], [14], fatorização de matrizes [4] e também algoritmos baseados em processos físicos de difusão de massa [15], [16], [17]. A seção seguinte apresenta em mais detalhes o algoritmo híbrido baseado em difusão de massa apresentado em [15], o qual ainda é explorado por pesquisas recentes envolvendo SR, e foi a base para o desenvolvimento da proposta desta pesquisa.

III. Algoritmos híbrido baseado em difusão

O algoritmo híbrido apresentado em [15] combina os algoritmos *Mass Diffusion(MD)* [18] e *Heat-Spreading(HS)* [19] para a geração das recomendações através de difusão de massa. A partir deste ponto, o mesmo será referenciado apenas como MD_HS.

Basicamente, neste algoritmo um SR é representado como um grafo bipartido, definido formalmente como $G = \{U, I, E\}$, onde $U = \{u_1, u_2, ..., u_N\}$, $I = \{i_1, i_2, ..., i_M\}$ e $E = \{e_1, e_2, ..., e_K\}$ são o conjunto de usuários, o conjunto de itens e o conjunto de arestas do grafo, respectivamente. Dado um conjunto de dados previamente conhecido, o grafo G é construído, atribuindo cada usuário a um vértice $u_i \in U$, cada item distinto a um vértice $i_j \in I$ e, caso o usuário u_i tenha tido qualquer interação com o item i_j, uma aresta $e_s \in E$ é inserida em G, o que torna u_i adjacente a i_j. Logo, para cada usuário alvo da recomendação (u) presente na base de dados, são executadas os três etapas a seguir:

Passo 1 Inicialmente, um valor de recurso $r(u,i)$ é atribuído a cada item i no grafo, da seguinte forma: se existe uma aresta entre i e u então $r(u,i) = 1$, caso contrário, $r(u,i) = 0$.

Passo 2 Na segunda etapa, ocorre um processo de propagação dos valores de recurso do lado item para o lado usuário no grafo; cada item i com $r(u,i) > 0$ propaga um novo valor de recurso recalculado $r'_{HB}(u,i)$ para cada usuário u com o qual é adjacente no grafo G.

Passo 3 Na última etapa do processo, ocorre uma nova propagação dos recursos do lado usuário para o lado item no grafo, onde cada item i recebe um valor de recurso recalculado $r''_{HB}(u,i)$ a partir dos valores de recurso do lado usuário, $r'_{HB}(u,i)$.

O cálculo dos novos valores de recurso nos Passos 2 e 3 descritos anteriormente dependem do algoritmo considerado - MD, HS ou MD_HS, além da quantia de interações que os usuários e itens tiveram na base de dados do SR, o que é representado pelo grau dos vértices no grafo, dado por $w(u)$ e $w(i)$, sendo respectivamente o grau do usuário u e do item i . Neste artigo, o cálculo destes valores de recurso é apresentado de forma resumida através das equações:

$$r'_{HB}(u,i) = (\sum_{i \in I} \frac{r(u,i)}{w(i)^{\lambda}})/w(u)^{(1-\lambda)}; \quad e \tag{1}$$

$$r''_{HB}(u,i) = (\sum_{u \in U} \frac{r'_{HB}(u,i)}{w(u)^{\lambda}})/w(i)^{(1-\lambda)}. \tag{2}$$

Nota-se que quando $\lambda = 0$ tem-se puramente a aplicação original do algoritmo HS e, quando $\lambda = 1$, tem-se a aplicação original do algoritmo MD. Qualquer valor entre 0 e 1 permite a combinação de ambos em MD_HS.Após a execução dos três passos descritos anteriormente, referentes ao usuário alvo u, todos itens com um valor final de recurso positivo, $r''(u,i) > 0$, são então ordenados de forma crescente, resultando na chamada lista de predição; sendo os itens com os maiores valores de recurso os que compõem a lista de recomendação.

Observe que o algoritmo MD tende a gerar recomendações compostas de itens mais populares (vértices do grafo com maiores graus), enquanto que HS tende a recomendar itens menos conhecidos (vértices de menores graus no grafo). Em [15], o mesmo grau de mistura ($\lambda = 0,5$) é utilizado para todo e qualquer usuário, independentemente de seu perfil.

IV. Difusão orientada ao perfil do usuário (algoritmo UPOD)

A proposta do presente mestrado consiste em um algoritmo capaz de combinar o MD_HS com o aprendizado supervisionado do grau de mistura (λ) em função do perfil individual de cada usuário, para permitir a geração de recomendações personalizadas através de difusão. O método foi nomeado como "Difusão orientada ao Perfil do Usuário"; ou *User Profile Oriented Diffusion (UPOD)*, em inglês. A ideia consiste em agrupar usuários que compartilhem perfis similares e definir,

para cada tipo de perfil, o valor de λ mais apropriado para o algoritmo MD_HS. Tal algoritmo é composto em fases, de treinamento e recomendação, apresentadas nas subseções a seguir.

A. Fase de Treinamento

Esta fase tem por objetivo a geração de um classificador treinado, capaz de predizer o grau de mistura mais adequado para determinado usuário tomando por base seus atributos, disponíveis em alguma base de dados (ex. gênero, idade e localização).

Todo o fluxo é exemplificado através dos passos descritos no algoritmo 1; inicialmente é criado um conjunto de treinamento vazio (passo 1); Na sequencia, no passo 2, a partir do grafo bipartido G_{train} um conjunto de usuários de treinamento U_{train} é criado, contendo os valores dos atributos $Feat$ para cada usuário de G. No passo 3, os usuários presentes em U_{train} são agrupado em k grupos menores através do algoritmo k-$Modes$, o qual consiste de uma extensão do algoritmo k-$Means$ para dados categóricos [20].

Para cada um dos k grupos de usuários resultantes (laço for, do passo 4 ao 10), calcula-se o melhor valor de λ (λ_{best}) através da função "MelhorLamda" no passo 5 (na prática, internamente são feitas execuções do algoritmo MD_HS e são medidos os melhores valores de λ para o cálculo das métricas do conjunto $Metric$). Para cada usuário de cada um dos k grupos são obtidos os valores de seus atributos individuais (passo 7) e é gerado o par <ValorAtributos, λ_{best} >, que é adicionado ao conjunto de treinamento no passo 8. Posteriormente este conjunto é utilizado para o treinamento do classificador no passo 11. Por fim, tem-se o classificador treinado a partir de todos os pares presentes no conjunto de treinamento; o classificador considerado foi o SVM [21]

Algorithm 1 Fase de Treinamento do UPOD

Require: grafo bipartido usuário-item de treinamento G_{train}, conjunto de atributos de usuário $Feat$, k, Λ, conjunto de métricas $Metric$
1: $CjTrain \leftarrow \{\}$
2: $U_{train} \leftarrow usuarios$(G$_{train}$, Feat)
3: $grupos[1..k] \leftarrow kModes(U_{train}, k)$
4: **for** $i = 1$ to $i = k$ **do**
5: $\lambda_{best}[i] \leftarrow MelhorLambda$(G$_{train}$, grupos[i], Λ,Metric)
6: **for** each usuário de grupos[i] **do**
7: $ValorAtributos \leftarrow ExtraiValor(grupos[i].user, Feat)$
8: $CjTrain \leftarrow CjTrain \cup \{< ValorAtributos, \lambda_{best}[i] >\}$
9: **end for**
10: **end for**
11: $classificador \leftarrow TreinaClassificador(CjTrain)$
12: **return** $classificador$

B. Fase de Recomendação

Esta fase é descrita no algoritmo 2: para cada usuário alvo u_a, são lidos seus atributos (passo 1), os quais são fornecidos como entrada para o classificador já treinado, que por sua vez fornece como saída a predição do valor de λ_{u_a} para o usuário u_a durante o passo 2. No passo 3, tendo como entradas o grafo bipartido de recomendação G_{rec}, o usuário alvo u_a, o valor predito λ_{u_a} e o tamanho da lista de recomendações L, UPOD aplica o algoritmo MD_HS (eq. 1 e 2) e fornece então uma lista de recomendação personalizada para u_a, levando em conta o valor de λ_{u_a}.

Algorithm 2 Fase de Recomendação do UPOD

Require: conjunto de atributos de usuários $Feat$,
usuário alvo da recomendação u_a,
$classificador$,
grafo bipartido usuário-item para recomendação G_{rec},
número de itens na lista de recomendação L.
1: $ValorAtributos \leftarrow ExtraiAtributos(u_a, Feat)$
2: $\lambda_{u_a} \leftarrow classificador(ValorAtributos)$
3: $listaRecomendacao \leftarrow$MD_HS(G$_{rec}$, u_a, λ_{u_a}, L)
4: **return** $listaRecomendacao$

UPOD foi avaliado de acordo com algumas métricas descritas na próxima seção.

V. Resultados Experimentais

Com o intuito de medir o quanto os itens recomendados correspondem ao que o usuário, de fato, gostaria de receber foram consideradas as seguintes métricas de avaliação:

- *Recall(Re(L))*: mede a proporção de itens relacionados ao usuário alvo no conjunto de validação que correspondem a itens na lista de recomendação gerada. Quanto maior seu valor, melhor o resultado.
- *Precision(Pe(L))*: mede a proporção de itens na lista de recomendação gerada que correspondem a itens relacionados ao usuário alvo no conjunto de validação. Portanto, quanto maior o valor desta métrica melhor o resultado.
- *RankScore(RS)*: leva em consideração a posição em que os itens aparecem na lista de recomendação gerada ao usuário. Na prática, calcula-se um valor de *rank* para cada item presente na lista, sendo que quanto mais próximos os itens estiverem das primeiras posições, menor será o valor total desta métrica e, portanto, melhor o seu resultado.

Para os experimentos foi considerado um subconjunto aleatório da base de dados LastFM [22], contendo 2.846 usuários, 4.995 itens e 14.583 interações entre ambos. Foram comparados os algoritmos colaborativo tradicional (FC), o algoritmo MD_HS e o algoritmo UPOD. Para todos algoritmos foram consideradas 10 execuções, sendo que a cada iteração houve uma divisão aleatória independente dos conjuntos de treinamento e validação, utilizados para a geração do grafo bipartido usuário-item no caso dos algoritmos MD_HS e *UPOD*. Foi considerado o particionamento da base de dados de forma a ter 80% para treinamento e 20% para validação, assim como nas pesquisas relacionadas ao algoritmo MD_HS. O tamanho adotado para as listas de recomendação em cada um dos algoritmos foi $|L| = 30$

Especificamente no caso do algoritmo UPOD, foi considerado o seguinte espaço de atributos para o agrupamento feito por $k - Modes$ sobre esta base de dados: idade, país (ex. "Germany") e gênero (m ou f). Para o atributo idade foram considerados intervalos de 2, 5, 10 e 20 anos (dependendo do intervalo escolhido, o atributo idade assumiria valores como "5_10" e "15_20", no caso de intervalo de 5 anos). A fase de treinamento do *UPOD* levou em conta k grupos, sendo $k \in \{2, 5, 10, 20, 30, 40, 50, 100, 200\}$. Note que foram feitos

experimentos variando tanto o intervalo de idade quanto k e, de forma experimental, chegou-se ao valor de $k = 5$ e intervalo de 20 anos de idade para esta base de dados. Na prática, esta configuração foi a que obteve os melhores resultados para UPOD, dentro das métricas avaliadas. Por fim, foi considerado o classificador SVM [21] para a fase de treinamento do UPOD.

A tabela a seguir exibe os resultados comparativos entre os algoritmos FC, MD_HS e UPOD para a base de dados LastFM.

Tabela I
RESULTADOS OBTIDOS PARA AS MÉTRICAS RECALL, PRECISION E RANKSCORE APÓS EXECUÇÃO NA BASE DE DADOS LASTFM.

Alg.	**Re(L)**		**Pe(L)**		**RS**	
	média	σ	média	σ	média	σ
FC	0.016	0.002	0.0011	0.0001	0.426	0.004
MD_HS	0.087	0.003	0.0064	0.0002	0.264	0.004
UPOD	**0,149**	**0,007**	**0,0105**	**0,0003**	**0,258**	**0,004**

Através dos resultados, observa-se que o algoritmo UPOD obteve resultados melhores que FC e MD_HS de acordo com as métricas consideradas. Foi aplicado o Teste t sob os resultados considerando grau de confiança igual a 95% ($\alpha = 0.05$) e $N = 10$ e comprovou-se superioridade estatística dos resultados de UPOD em relação aos obtidos pelos demais algoritmos (resultados em negrito).

VI. CONCLUSÃO E TRABALHOS FUTUROS

Este artigo apresentou o algoritmo UPOD, o qual permite determinar automaticamente o grau de mistura no processo de difusão para a geração de recomendações personalizadas, em função do perfil particular de um usuário. Demonstrou-se através de alguns experimentos em uma base de dados esparsa que este algoritmo pode melhorar a qualidade das recomendações quando comparado aos algoritmos FC e MD_HS. Como próximos passos, visando aprimorar os resultados do algoritmo UPOD, pretense-se executá-lo sob uma base de dados sintética altamente esparsa e com um número maior de atributos de usuários, assim como permitir um maior número de propagações no grafo bipartido durante as recomendações.

AGRADECIMENTOS

Gostaríamos de agradecer ao CNPq (Proc. N. 425860/2016-7 e N. 307027/2017-1) e à FAPESP (Proc. N. 2016/21047-3).

REFERÊNCIAS

[1] KOTKOV, D.; WANG, S.; VEIJALAINEN, J. A survey of serendipity in recommender systems. *Knowledge-Based Systems*, Elsevier B.V., v. 111, p. 180–192, 2016. ISSN 09507051. Disponível em: <http://dx.doi.org/10.1016/j.knosys.2016.08.014>.

[2] BOBADILLA, J. et al. Recommender systems survey. *Knowledge-Based Systems*, Elsevier B.V., v. 46, p. 109–132, 2013. ISSN 09507051. Disponível em: <http://dx.doi.org/10.1016/j.knosys.2013.03.012>.

[3] SANCHEZ-MORENO, D. et al. A collaborative filtering method for music recommendation using playing coefficients for artists and users. *Expert Systems with Applications*, v. 66, p. 1339–1351, 2016. ISSN 09574174.

[4] YANG, Z. et al. A Survey of Collaborative Filtering-Based Recommender Systems for Mobile Internet Applications. *IEEE Access*, v. 4, p. 3273–3287, 2016. ISSN 2169-3536.

[5] LACERDA, A. Multi-Objective Ranked Bandits for Recommender Systems. *Neurocomputing*, Elsevier B.V., v. 0, p. 1–13, 2017. ISSN 09252312. Disponível em: <http://linkinghub.elsevier.com/retrieve/pii/S092523121730228X>.

[6] LU, J. et al. Recommender system application developments: A survey. *Decision Support Systems*, Elsevier B.V., v. 74, p. 12–32, 2015. ISSN 01679236. Disponível em: <http://dx.doi.org/10.1016/j.dss.2015.03.008>.

[7] LU, Z. et al. Content-based collaborative filtering for news topic recommendation. *AAAI 2015: Proceedings of the Twenty-ninth AAAI Conference on Artificial Intelligence*, p. 217–223, 2015.

[8] ZHANG, S.; YAO, L.; SUN, A. Deep Learning based Recommender System: A Survey and New Perspectives. *ACM Journal on Computing and Cultural Heritage (JOCCH)*, v. 1, n. 1, p. 1–35, 2017. ISSN 15232867. Disponível em: <http://arxiv.org/abs/1707.07435>.

[9] CHRISTAKOPOULOU, E.; KARYPIS, G. Local Item-Item Models For Top-N Recommendation. *Proceedings of the 10th ACM Conference on Recommender Systems - RecSys '16*, p. 67–74, 2016. Disponível em: <http://dl.acm.org/citation.cfm?doid=2959100.2959185>.

[10] MORADI, P.; AHMADIAN, S. A reliability-based recommendation method to improve trust-aware recommender systems. *Expert Systems with Applications*, Elsevier Ltd, v. 42, n. 21, p. 7386–7398, 2015. ISSN 09574174. Disponível em: <http://dx.doi.org/10.1016/j.eswa.2015.05.027>.

[11] PEARSON, K. Notes on the History of Correlation. v. 13, n. 1, p. 25–45, 1920.

[12] SHAMBOUR, Q.; LU, J. An effective recommender system by unifying user and item trust information for B2B applications. *Journal of Computer and System Sciences*, Elsevier Inc., v. 81, n. 7, p. 1110–1126, 2015. ISSN 00220000. Disponível em: <http://linkinghub.elsevier.com/retrieve/pii/S0022000014001998>.

[13] HORSBURGH, B.; CRAW, S.; MASSIE, S. Learning pseudo-tags to augment sparse tagging in hybrid music recommender systems. *Artificial Intelligence*, Elsevier B.V., v. 219, p. 25–39, 2015. ISSN 00043702. Disponível em: <http://dx.doi.org/10.1016/j.artint.2014.11.004>.

[14] ZHOU, Y.; ZENG, A.; WANG, W. H. Temporal effects in trend prediction: Identifying the most popular nodes in the future. *PLoS ONE*, v. 10, n. 3, p. 1–10, 2015. ISSN 19326203.

[15] ZHOU, T. et al. Solving the apparent diversity-accuracy dilemma of recommender systems. *Proceedings of the National Academy of Sciences of the United States of America*, v. 107, n. 10, p. 4511–4515, 2010. ISSN 0027-8424.

[16] WANG, X. et al. Mixed Similarity Diffusion for Recommendation on Bipartite Networks. *IEEE Access*, v. 5, p. 21029–21038, 2017. ISSN 21693536.

[17] DENG, X. et al. A general and effective diffusion-based recommendation scheme on coupled social networks. *Information Sciences*, Elsevier Inc., v. 417, n. 168, p. 420–434, 2017. ISSN 00200255. Disponível em: <http://dx.doi.org/10.1016/j.ins.2017.07.021>.

[18] ZHOU, T. et al. Bipartite network projection and personal recommendation. *Physical Review E - Statistical, Nonlinear, and Soft Matter Physics*, v. 76, n. 4, p. 1–7, 2007. ISSN 15393755.

[19] ZHANG, Y.-C.; BLATTNER, M.; YU, Y.-K. Publisher's Note: Heat Conduction Process on Community Networks as a Recommendation Model [Phys. Rev. Lett. 99, 154301 (2007)]. *Physical Review Letters*, v. 99, n. 16, p. 169902, 2007. ISSN 0031-9007. Disponível em: <http://link.aps.org/doi/10.1103/PhysRevLett.99.169902>.

[20] HUANG, Z. Extensions to the k -Means Algorithm for Clustering Large Data Sets with Categorical Values. v. 2, n. 3, p. 283–304, 1998.

[21] WITTEN, I. H. et al. Weka: Practical machine learning tools and techniques with Java implementations. In: KASABOV, N.; KO, K. (Ed.). *Proceedings of the ICONIP/ANZIIS/ANNES'99 Workshop on Emerging Knowledge Engineering and Connectionist-Based Information Systems*. [S.l.: s.n.], 1999. p. 192–196. Dunedin, New Zealand.

[22] CELMA, O. *Music Recommendation and Discovery in the Long Tail*. [S.l.]: Springer, 2010.

Towards 5G: A Projection of Autonomous Networks Supported by Cloud & Edge Computing
Rumo ao 5G: Uma Projeção de Redes Autônomas Suportadas por Computação em Nuvem

OLIMPIO, J.*; CUGNASCA, C.*; MARTUCCI, M.†
*Programa de Pós-Graduação em Engenharia Elétrica
†Escola Politécnica da USP – Engenharia de Computação e Sistemas Digitais
E-mail: olimpio.rodrigues@usp.br, carlos.cugnasca@usp.br, mmartucc@usp.br

***Abstract*—With the advent of Internet of Things, Internet traffic and applications have grown considerably, which presupposes that telecommunications and computing networks have to adapt to this new reality due to the characteristic challenges in terms of the current limitations of such networks front new demands. Ahead of its time, this article thus presents a study for the projection of data communications networks together with a new model of computational processing towards the futuristic requirements of the Fifth Generation of Mobile Networks, 5G.**

***Keywords*— Internet of Things, Real Time, Big Data, Edge Computing, Cloud Computing, Software Defined Networking, Artificial Intelligence, 5G, Latency**

***Resumo*— Com o advento da Internet das Coisas, as aplicações e tráfego de Internet têm crescido bastante, o que pressupõe que as redes de telecomunicações e computação tenham de se adequar a essa nova realidade, haja vista os desafios característicos em termos de limitações atuais dessas redes frente às novas demandas. À frente de seu tempo, este artigo, assim, traz um estudo de projeção das redes de comunicações de dados juntamente com um novo modelo de processamento computacional rumo às exigências futurísticas da Quinta Geração de Redes Móveis, 5G.**

***Palavras-chave*— Internet das Coisas, Tempo Real, *Big Data*, Computação de Borda, Computação em Nuvem, *Software Defined Networking*, Inteligência Artificial, 5G, Latência**

***Classificação*— Mestrado**

***Categoria*— Iniciante**

I. Introdução

A IoT (Internet das Coisas) [4] é um conceito criado em 1.999 por Kevin Ashton no *Massachusetts Institute of Technology* que vem sendo amplamente estudado, o qual se trata de um paradigma que preconiza um mundo de objetos físicos moldando uma rede de objetos inteligentes capazes de realizar processamentos, capturar variáveis ambientais e reagir a estímulos externos, conectados à Internet, interconectando-se entre si e com outros recursos (físicos ou virtuais) [1]. Entretanto, para que os milhares de dispositivos de IoT possam funcionar adequadamente, são necessárias profundas transformações nos modelos atuais de comunicações e processamentos, pois, a cada dia, surgem desafios que satisfaçam novos critérios de funcionamento para a sua implementação,

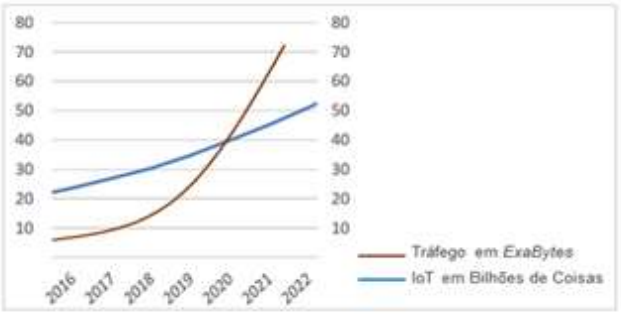


Fig. 1. Fonte: Adaptado de [5]. Projeção do crescimento de tráfego mundial Internet e do número de dispositivos IoT

principalmente no que diz respeito à questão de conectividade, por exemplo, para os objetos de detecção e atuação com os sistemas embarcados e que trabalham em tempo real.

Para se ter uma dimensão do aumento da quantidade de tráfego Internet, a figura 1 mostra claramente o crescimento esperado no tráfego de Internet mundial e no número de objetos conectados à Internet.

Neste sentido, deverá ser disponibilizado um processamento computacional realmente eficiente, o qual não poderá apenas ser feito em camadas superiores como em *Cloud Computing* ou Computação em Nuvem, mas sim em borda, o chamado *Edge Computing*, haja visto, por exemplo, o requerimento de baixa latência demandada por diversos sistemas.

Dessa forma, a computação de borda pode ser entendida como uma otimização da computação em nuvem, através do processamento dos dados mais próximos das fontes dos dados do que na computação em nuvem propriamente dita, ou seja, temos que a combinação de IoT e computação de borda [6] constitui o cenário adequado ao que se espera rumo a novas conexões de Internet. O principal objetivo da computação de borda é estender as funções de computação em nuvem para as bordas da rede. Devido à proximidade com os usuários finais e sua implantação descentralizada, ela pode suportar com qualidade os aplicativos e serviços que exigem os requisitos

de baixa latência, alta mobilidade com reconhecimento de localização.

Por outro lado, o desenvolvimento do 5G trata-se de um tema de grande importância, o qual não é apenas uma simples evolução das tecnologias em telecomunicações e será potencialmente aplicável em diversos campos de utilizações a nível mundial, haja vista a necessidade cada vez maior de velocidades e menores latências [3] dos dispositivos de telecomunicações, que impulsionará uma rápida e inumerável adoção de soluções de IoT com transformações profundas em diversas indústrias, além de possibilitar o surgimento de novos modelos de negócios a níveis hospitalar, agropecuário, trânsito de veículos etc. A latência requerida em redes 5G deverá ser de até 1 ms (milissegundo) nos centros urbanos.

No 5G, todos os tipos de recursos, como comunicação, computação e armazenamento em *cache*, distribuir-se-ão pela rede, sendo um desafio importante coordenar esses recursos para a sua utilização efetiva no tratamento da enorme quantidade de dados distribuídos. Além da baixa latência e dados de posicionamento, a plataforma IoT emergente requer também o suporte para mobilidade contínua e cobertura onipresente que não pode ser totalmente suportado por soluções de computação em nuvem tradicional. O principal desafio é como lidar com o processamento em tempo real de uma enorme quantidade de dados e informações, chamados *big data*, gerados a partir de dados heterogêneos que vêm dos ambientes de IoT.

Assim, para uma distribuição eficiente de análises de IoT e uso de recursos de rede, faz-se necessária uma coordenação entre a plataforma analítica de IoT e a infraestrutura de nuvem por uma Rede Definida por *Software* (SDN) [2]. Dentro de um ambiente SDN, um único controlador ou grupo de controladores poderá fornecer serviços de plano de controle de encaminhamento de dados para um maior número de nós, permitindo assim uma visão de todo o sistema de recursos de rede. O SDN possibilita que os dados sejam encaminhados dinamicamente, em uma base de fluxo por fluxo, usando informações de origem e de destino, o que proporciona melhores velocidades e latência e elimina possíveis gargalos comuns nas arquiteturas atuais. O *OpenFlow*, protocolo que fornece uma camada de abstração da rede física para o elemento de controle, permite que a rede seja configurada ou manipulada através de *software*, ou seja, trabalha harmonicamente com a tecnologia SDN.

É relevante também o desenvolvimento de técnicas para converter uma enorme quantidade de dados brutos em informação significativa no *big data*. As técnicas de aprendizado de máquina visam a criar um relacionamento funcional entre o conjunto de dados de entrada e as ações de saída, e são capazes de executar previsões e decisões com base nos dados de entrada sem exigir a necessidade de seguir instruções do programa estático. Com base no tempo de processamento necessário para a análise de *big data*, estas técnicas potenciais podem ser classificadas de maneira geral em processamento por fluxo ou por lote.

Neste sentido, assim como os veículos autônomos do futuro, capazes de serem dirigidos sem a intervenção humana, as

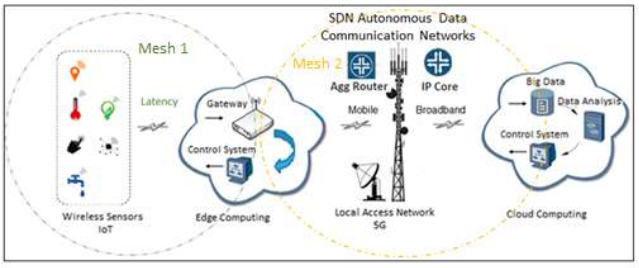


Fig. 2. Fonte: Adaptado de [3]. Topologia básica da estrutura computacional e rede autônoma para atendimento IoT no 5G

redes de comunicação de dados rumo ao 5G tendem a ser igualmente autônomas [5]. Estas redes, então, tendem também a ser trabalhadas com Inteligência Artificial (IA) sob análises avançadas. Isto exige, inicialmente, uma combinação coerente de inteligência com controle e supervisão humana, processos operacionais automatizados, controlados por *software* e infraestrutura programável subjacente para que possam se adaptar, autoconfigurar, automonitorar, autoreparar e autootimizar por meio de avaliação constante das mudanças na rede e de realocação automática de recursos.

Essas redes programáveis e autônomas, portanto, usarão recursos de aprendizado de máquina e otimização para se adaptarem dinamicamente às demandas de serviço e aos padrões de tráfego. Dessa forma, o controle por *software*, que consiste na base das operações adaptativas, possibilitará a criação e a implantação dos serviços automatizados em redes autônomas sob as necessidades e velocidades programadas.

Existe, pois, uma lacuna de pesquisa interessante a ser preenchida com a seguinte questão: qual arquitetura de rede de dados poderá, efetivamente, contribuir para um melhor aproveitamento da conectividade em 5G?

II. Objetivos

Os objetivos deste trabalho são:

- Geral: Apontar um modelo sumarizado de rede de comunicação de dados autônoma que possa ser aderente aos requisitos do 5G diante no que tange à questão de baixa latência, tornando a contribuição deste trabalho significativa rumo aos melhores desempenhos em 5G;
- Específico: Simular uma rede *ad-hoc* com e sem a tecnologia de SDN para validar a melhoria da latência com a utilização do SDN e suportar o objetivo geral aqui proposto.

III. Proposição da Solução

A. Metodologia

A metodologia empregada para se alcançar os objetivos deste trabalho foi realizada sob premissa de pesquisas de caráter exploratório, descritivo e empírico, através de simulações laboratoriais e análises das informações e resultados encontrados sob dois cenários estudados. Foi utilizado, para tanto, o COOJA (COntiki Os JAva), um simulador/emulador de rede de sensores sem fio que permite

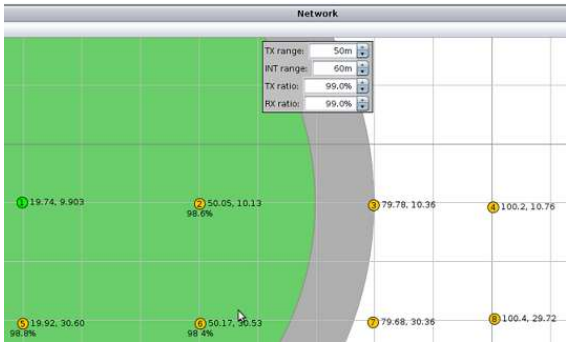


Fig. 3. Topologia sem SDN com detalhe das coordenadas x,y dos nós. Nó 1 é o *sink*

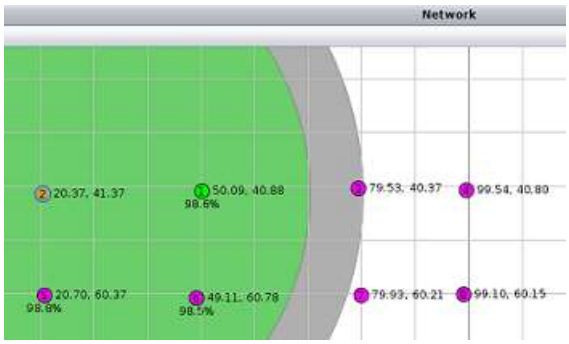


Fig. 4. Topologia com SDN com detalhe das coordenadas x,y dos nós. Nó 1 é o controlador e Nó 2, o *sink*

a emulação de plataformas de *hardware* reais. Para efeito de análise da latência e facilitar o entendimento, parte-se da topologia apresentada na figura 2, através da simulação do comportamento apenas da malha 1 (*mesh 1*) em rádio-propagação. As topologias realizadas nas simulações no COOJA seguem nas figuras 3 e 4, caracterizando-se por representarem dois ambientes similares de IoT com nós-sensores e 1 (um) *sink*, porém sem e com SDN, respectivamente, o que impactará nos resultados alcançados. A tabela I mostra as configurações das simulações. Os *softwares* utilizados foram: COOJA v1.8, QT Creator v5.8, Instant Contiki v3.0, it-SDN v0.3, sob VMware v14 e Ubuntu v18.04.

Pretende-se, com as simulações, fazer o levantamento dos tempos de latência e taxa de entrega de pacotes das redes sem e com SDN ora expostas nas topologias 3 e 4, sob diferentes usos de encaminhamento de pacotes.

B. Resultados e Análises

A figura 5 expressa os resultados obtidos, a partir dos quais, tem-se que:

- O ibc (*Identified Best-effort Single-hop Broadcast*) não se trata de um protocolo propriamente dito, caracterizando-se por, apenas, permitir o envio de pacotes aleatoriamente (*broadcasting*) a seus vizinhos, isto é, não realizando roteamento de dados, então, apesar da baixa latência (1 ms), é bastante propício a perdas de pacotes na rede (43% entregues) e, por consequência, à elevação de consumo energético dos nós;
- Os protocolos CTP (*Collection Tree Protocol*), que computa e mantém rotas para um ou mais sorvedouros, construindo e mantendo árvores de custo mínimo com o sorvedouro como raiz e RPL (IPv6 *Routing Protocol for Low-Power and Lossy Networks*), que constrói um grafo acíclico dirigido orientado a destino para endereçar os pacotes, são capazes de rotear dados, apresentando resultados melhores de entregas de pacotes do que com ibc (98% e 99%, respectivamente), porém com a utilização da tecnologia de SDN (*Software Defined Networking*), uma abordagem de arquitetura de rede que permite controlar ou "programar" a rede de maneira central e melhor usando aplicativos de *software*, haverá um controle centralizado e otimizado das redes WSN, inclusive também em cenários de IoT, traduzindo-se em alta taxa de entrega (99%) e latência menor (56 ms) do que em CTP e RPL sem SDN (107 e 132 ms, respectivamente).

TABELA I
PARÂMENTOS DAS SIMULAÇÕES

Item	Atribuição
Métricas	Latência e Taxa de Entrega
Topologia	"Grade", *Sink* à esquerda superior
TX Range/INT Range	50m/60m
Taxa de Sucesso TX/RX	99%/99%
Tempo de cada simulação	12 minutos
Velocidade de cada simulação	100%
Tipo de Nós	Tmote Sky; Estáticos
Número de Nós-Fontes	7 ou 6 (SDN)
Número de Nós-Sinks	1
Tipo de Nós	Tmote Sky; Estáticos
"Protocolos" Utilizados	ibc; CTP, RPL
Camada MAC	CSMA
RDC	NullRDC
CCR	128Hz
Modelo de Rádio-Propagação	UDGM Perda em Distância
Camada Física	IEEE 802.15.4

Fig. 5. Resultados: Taxa de Entrega e Latência

C. Modelo de Rede Computacional

Diante do exposto, aponta-se uma nova estrutura para processamento coordenado entre computação de borda e nuvem, integrando vantagens de ambas as plataformas com a

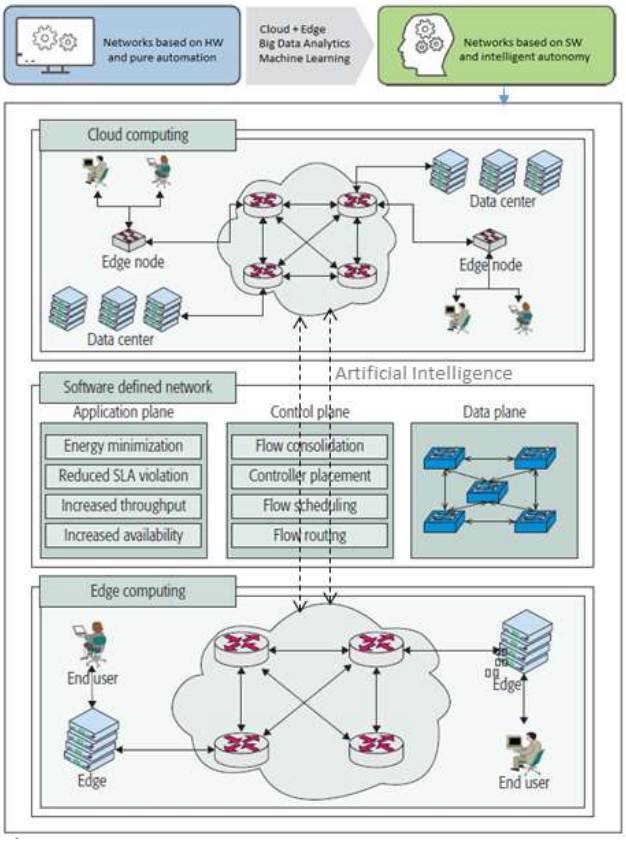


Fig. 6. Fonte: Adaptado de [2]. Modelo de Rede Autônoma Suportada por Computação em Nuvem

orquestração em *software*. A figura 6 explora o conceito proposto a partir da malha 2 (*mesh* 2) da figura 2 levando à infraestrutura programável, ou seja, uma **rede autônoma**, híbrida, de última geração composta de redes físicas abertas e habilitadas por SDN e funções virtualizadas em nuvem, o que oferecerá telemetria avançada e dados em tempo real sobre a integridade da rede, além de ajustes rápidos para atender às diferentes necessidades, e à inteligência orientada por análise, que possibilita a automação inteligente, aprimorando a tomada de decisões (autônomas), oferecendo suporte ao controle por *software* através de mecanismos de políticas, IA, aprendizado de máquina e telemetria.

O controle por *software* em uma rede autônoma inclui a orquestração da rede em vários domínios. Outro aspecto importante que pode ser explorado na estrutura proposta é que o processamento em nuvem pode utilizar as informações de histórico disponíveis no centro da nuvem para inferir certas decisões para o processamento de borda sem a necessidade de aguardar os dados instantâneos coletados dos nós em IoT, o que certamente reduzirá a latência.

IV. Conclusão e Trabalhos Futuros

Há, atualmente, restrições técnicas nos modelos das redes de comunicações de dados quanto às taxas computacionais, tamanhos dos *caches*, larguras de banda de comunicação e latências diante do volume de tráfego esperado no futuro. Visto que as pesquisas sobre *edge computing*, IoT e 5G se popularizam, mas ainda estão incipientes quanto ao caráter de mensurar com precisão os reais benefícios de uma computação eficiente em nível de borda, o tema ora apresentado e discutido neste trabalho se torna relevante no tange, principalmente, à demanda de baixa latência do 5G.

A computação em nuvem convencional não é adequada para aplicativos que exigem baixa latência, operação em tempo real e alta qualidade de serviços; já a computação de borda é adequada para tais aplicativos e ao suporte de mobilidade e reconhecimento de local ou contexto, mesmo que eles não tenham recursos suficientes de armazenamento. Considerando tais aspectos, este artigo apontou uma nova estrutura de processamento em nuvem para permitir a análise de dados em tempo real em redes de IoT. A introdução da computação de borda sobre a computação em nuvem centralizada traz oportunidades para equilibrar o *trade-off* entre arquiteturas de rede centralizadas e distribuídas.

Considera-se que a latência seja minimizada com uma infraestrutura de controlador SDN P2P (*peer-to-peer*) ou distribuída, por partilhar a carga de comunicação do controlador, o que foi simulado neste trabalho em P2P e cujos objetivos foram alcançados. Mais ainda, para menores latências, é necessária a orquestração das computações em nuvem via o controle por *software* em redes autônomas distribuídas e inteligentes. A autonomia da rede não trará apenas melhor latência, mas sim outros muitos benefícios técnico-comerciais aos usuários e provedores.

Na plataforma de rede autônoma apontada, várias técnicas de processamento de dados assistidas por nuvem, como filtragem de dados, compressão e técnicas de extração de recursos, detecção/monitoramento, codificação/decodificação distribuída, combinações e tomada de decisão, assim como execução de cálculos no lado da nuvem nos dados de IoT criptografados sem perda de privacidade, como garantir que os dados não sejam corrompidos no trânsito do processamento de borda para o centro da nuvem, e como executar tarefas da borda à nuvem de maneira segura precisam ser endereçadas e pesquisadas, para que tal apontamento de rede autônoma possa efetivamente contribuir de maneira tão sólida às melhorias dos processos de comunicações quanto necessário.

Referências

[1] ATZORI, L.; LERA, A.; MORABITO, G. The Internet of Things: A survey. *Computer Networks*, v. 54, n. 15, p. 2787-2805, 2010.

[2] KAUR, K. et al. Edge Computing in the Industrial Internet of Things Environment: Software-Defined-Networks-Based Edge-Cloud Interplay. *IEEE Communications Magazine*, v. 56, n. 2, p. 44-51, fev. 2018. ISSN 1558-1896.

[3] PARVEZ, I. et al. A Survey on Low Latency Towards 5G: RAN, Core Network and Caching Solutions. *IEEE Communications Surveys and Tutorial*, 2017.

[4] PERERA, C. et al. Context aware computing for the Internet of Things: A survey. *IEEE Communications Surveys and Tutorial*, v. 16, n. 1, p. 414-454, 2013. ISSN 1553-877X.

[5] SANDANO, I. The Self-Driven Network In: *A trajetória rumo à automação e seus estágios*. São Paulo, Brasil, 2018.

[6] SHI, W. et al. Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal*, v. 3, n. 5, p. 637-646, 2016. ISSN 2372-4662.

Modeling Strategies for Bidimensional Climatic Data: Case Study on ARM

Estratégias de Modelagem de Dados Climáticos Bidimensionais: Um Estudo de Caso no ARM

BARBOSA, W. L.[†] ; KRISHNA, B.[¥]; ALVES-SOUZA, S.N.[†] ; CORREA, P. L. P. [†]
[†] Escola Politécnica - Universidade de São Paulo
[¥] Oak Ridge National Laboratory
wesleyloubar@usp.br, krishnab@ornl.gov, ssouza@usp.br, pedro.correa@usp.br

Abstract— **Climatic observations collected by ARM sensors need to be modeled to be provided for climate studies. The objective of this work is to compare the performance of simple and wide-column table structures in Cassandra in the modeling of two-dimensional climate data. A case study of an ARM data stream was used to verify the behavior of each strategy in three different insertion scenarios and, subsequently, the efficiency of the queries performed. The first strategy presented better performance in the insertion, while the second one in the data query. However, it is worth mentioning that more analysis needs to be done on other types of databases.**

***Keywords*— climatic data; Cassandra; modeling.**

Resumo — ***Observações climáticas coletadas por sensores da ARM precisam ser modeladas para serem fornecidas para estudos climáticos. O objetivo deste trabalho é comparar o desempenho de estruturas de tabelas simples e de wide-column no Cassandra na modelagem de dados climáticos bidimensionais. Um estudo de caso de um fluxo de dados ARM foi utilizado para verificar o comportamento de cada estratégia em três cenários diferentes de inserção e posteriormente, eficiência das consultas realizadas. A primeira estratégia apresentou melhor desempenho na inserção, enquanto a segunda na consulta de dados. No entanto, vale ressaltar que mais análises precisam ser feitas em outros tipos de bancos de dados.***

***Palavras-chave*— dados climáticos; Cassandra; modelagem.**
Classificação*—*Mestrado.
Categoria*—*Iniciante.

I. INTRODUÇÃO

As condições climáticas influenciam praticamente todas as atividades humanas. Em todo o mundo, diferentes equipes de cientistas estão estudando e criando modelos para projetar as condições climáticas futuras sob vários cenários para o próximo século [1]. Os resultados desses modelos projetam não somente como a temperatura global se comportará no próximo século, mas mostram que as decisões e o comportamento humanos que escolhemos hoje determinarão a dramaticidade do clima no futuro [2]. Modelos nos ajudam a trabalhar com problemas complicados e entender sistemas complexos como o clima.

Segundo [3], a pesquisa científica desempenha um papel crucial na abordagem de problemas ambientais globais, como mudanças climáticas, perda de biodiversidade e etc. Os avanços nesses campos dependem fortemente da disponibilidade de dados, permitindo que os pesquisadores entendam melhor os processos ambientais. De registros de temperatura obtidos usando termômetros simples, a medições complexas de sensores de satélite, a coleta de dados é uma componente chave de qualquer projeto de pesquisa [4]. No entanto, a coleta de dados é geralmente complexa, cara e demorada. Por isso, surgiram algumas iniciativas que buscam prover dados climáticos à comunidade científica de modo que estas possam continuar a testar teorias e soluções, para explorar e entender como os fenômenos climáticos funcionam. O Atmospheric Radiation Measurement (ARM) é um deles.

Criado pelo Departamento de Energia (Department of Energy - DOE) dos EUA em 1991, o ARM é uma iniciativa que visa implementar uma série de plataformas instrumentadas que fornecem uma base de observação para o estudo do clima da Terra. Cientistas utilizam dados coletados pelo ARM como transferência de calor por radiação, processos de aerossol e processos em nuvem, para desenvolver uma compreensão preditiva robusta do clima da Terra e sistemas ambientais [7].

Dada a complexidade de estudos climáticos, é vital que eles sejam baseados nas melhores evidências disponíveis. A provisão de dados climáticos é fundamental para permitir que os cientistas reúnam todas a peças necessárias para modelagem do comportamento climático no mundo [5]. Além da aquisição de dados, critérios técnicos de armazenamento e consulta são partes importantes para o processo de disponibilização de dados climáticos para promoção de um melhor entendimento, previsão e validação de modelos climáticos baseados em dados temporalmente apropriados. Assim, este trabalho procura analisar e comparar diferentes abordagens de modelagem de dados climáticos bidimensionais com relação ao desempenho de inserção e leitura de dados no Banco de Dados NoSQL Cassandra, utilizando diferentes abordagens implementadas na linguagem Python para testar se o modelo de dados definido consegue responder adequadamente e eficientemente as consultas executadas. A princípio acredita-se

que a extração dos dados utilizando o formato CSV (*Comma-separated Values*) apresenta melhor desempenho para a carga dos dados em uma estrutura de tabela simples, porque o comando COPY FROM interno do CQL (*Cassandra Query Language*) é útil e eficiente para a inserção de uma considerável quantidade de dados a partir de um formato de arquivo delimitado por vírgula [6].

O próximo tópico detalha a abordagem metodológica com os resultados sendo apresentados no tópico III. O tópico IV trás o fechamento do trabalho.

II. METODOLOGIA

O trabalho de pesquisa aqui apresentado caracteriza-se como um estudo de caso sobre a modelagem de dados climático bidimensionais. Estudos de casos, de acordo com [8], compõem um tipo importante de pesquisa que permite uma análise aprofundada sobre fenômenos pouco claros, enquanto trata de características holísticas e significativas de eventos reais. Embora não responda completamente a uma pergunta, um estudo de caso dará algumas indicações e permitirá a elaboração e criação de hipóteses sobre um determinado assunto [9].

A. *Fonte dos Dados*

Os dados utilizados para este trabalho caracterizam-se como dados temporais, por serem capturados em intervalos regulares ao longo do tempo. Eles são coletados por instrumentos do ARM no sítio *Southern Great Plains* (SGP), localizado em Oklahoma nos Estados Unidos. O SGP é o maior sítio e a mais extensa instalação de pesquisa climática do mundo e coleta dados sobre processos atmosféricos, de nuvens e aerossóis [10]. O ARM alocou mais de 50 plataformas de instrumentos no observatório do SGP, incluindo: radiômetros, radares, liDARs, instrumentação meteorológica de superfície, instrumentação para amostragem de aerossol, ceilômetros e radiossondas. Os dados utilizados no trabalho foram do instrumento radar, do nível C1. Dentro do SGP existe um grande número de instrumentos cujas medições são armazenadas em diferentes fluxos de dados. O fluxo de dados escolhido foi o sgpkazrge.C1 com um volume de dados de 1.2 *terabytes*.

B. *Características dos Dados*

O fluxo de dados sgpkazrge.C1 possui mais de 2500 arquivos, cada arquivo corresponde a um dia completo de observações, resultando em mais de 7 anos de dados coletados, entre 2011 e 2018. Os arquivos apresentam entre 200 e 800MB de volume e estão armazenados no formato de dados científicos NetCDF. Os dados em NetCDF são comumente empregados em organizações que trabalham com dados astronômicos, climáticos e ambientais.

Um arquivo NetCDF armazena dados em formato matricial e apresenta três componentes básicos: variáveis, atributos e dimensões. As variáveis são utilizadas para armazenar os dados coletados, de acordo com o tipo do dado (inteiro ou decimal). Os atributos representam os metadados associados a alguma variável, detalhando-a ou informando a unidade de medida. As dimensões são utilizadas para representar alguma dimensão física usada na captura do dado como tempo e altura.

Os arquivos NetCDF utilizados apresentavam 30 atributos, 24 variáveis e, entre essas variáveis, 16 eram unidimensionais e 8 eram bidimensionais. De acordo com [11], uma variável coletada em um único local em vários momentos é armazenada como uma matriz unidimensional, ao passo que uma variável coletada em vários locais em um único ponto no tempo é armazenada como uma matriz bidimensional. Nos dados utilizados neste trabalho, uma variável bidimensional apresentava 680 medições para cada intervalo de tempo. O intervalo de granularidade de tempo dos arquivos era de 3,7032286 segundos, resultando em 23.385 amostras coletadas por dia. Considerando 16 variáveis unidimensionais com 23.385 amostras por dia, e 8 variáveis bidimensionais com a mesma quantidade de amostras diárias, em que cada uma era coletada em 680 ranges diferentes, cada arquivo apresentava, portanto, 127.588.560 células de dados.

C. *Modelo de Dados*

A necessidade de se modelar dados climáticos no Cassandra partiu do interesse do ARM em testar uma interface de filtragem de dados para os usuários, permitindo que eles selecionassem os dados de interesse de acordo com critérios definidos como intervalo de tempo e range dos dados. O modelo de dados deveria ser capaz de responder à seguintes requisições:

1 – Retornar dados dentro de um range específico;
2 – Retornar dados dentro de um intervalo de tempo específico;
3 – Retornar dados com valores acima ou abaixo de um parâmetro definido.

O maior desafio foi criar um modelo de dados que atendesse os requisitos exigidos para a requisição dos dados, dada as características de modelagem do próprio Cassandra. A estratégia de modelagem empregada foi baseada em uma adaptação de [12], que propõe um novo modelo de dados para o Apache Cassandra baseado em consultas.

[12] propõe a utilização de um modelo de dados conceitual e o mapeamento para um modelo de dados lógicos com base em consultas definidas para a aplicação. Para o fluxo de dados considerado nesta análise, testaram-se três diferentes estratégias de carga de dados: Pandas, Batch e Excel, que são detalhadas à frente. As consultas definidas anteriormente podem ser realizadas pelos dois modelos de tabela esboçados na Figura 1 a seguir:

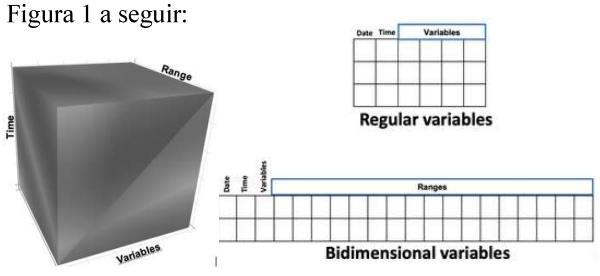


Fig. 1. Modelos de tabelas

A etapa final da metodologia adotada é a análise e a otimização de um modelo de dados lógicos para produzir um modelo de dados físico correto e eficiente. No caso do Cassandra, características próprias da modelagem do banco, conforme apresentado por [13], envolvem a escolha de chaves compostas para garantir o balanceamento da carga de dados em cada partição e o ordenamento dos dados. Esses aspectos são definidos pelas chaves de partição e ordenação, respectivamente, que em conjunto formam a chave primária. Assim, para o modelo definido na modelagem dos dados climáticos adotou-se dia, mês e ano como chaves de partição composta, e horário (time) como chave de ordenação.

Após a definição dos modelos de dados a serem testados, empregaram-se diferentes estratégias para transferência e carga dos dados extraídos dos arquivos em NetCDF para a base de dados criada no Cassandra. A primeira delas foi o uso de um Pandas *dataframe* do Python. O Pandas é uma biblioteca do Python que provê estruturas em forma de tabela ou planilha de dados que podem ser usadas para agrupar e agregar dados de maneira dinâmica [14]. No caso de um conjunto de dados de série temporal, os rótulos das linhas podem ser valores de data e hora, por exemplo. A segunda estratégia utilizada foi o uso do comando Batch do CQL do próprio Cassandra. O Batch é um comando interno do Cassandra para carga de dados direcionados a uma única partição, usado com o intuito de reduzir o tráfego cliente-servidor. Por fim, testou-se o uso de um arquivo CSV para ser importado para uma tabela existente no Cassandra empregando o comando COPY FROM.

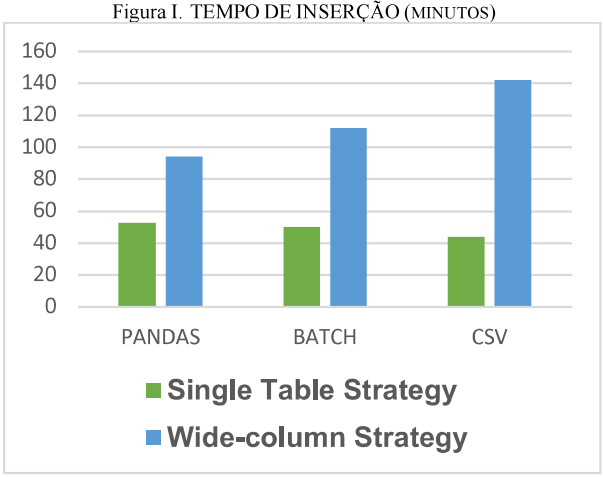
Os critérios utilizados para a comparação e verificação dos dois modelos propostos foram tempo de gravação e leitura dos dados, e eficiência da consulta (query) executada. Os resultados da análise serão apresentados no próximo tópico.

III. Resultados e Discussão

A modelagem dos dados é uma parte importante para a provisão efetiva e eficiente de dados científicos para os pesquisadores. Um dos propósitos do ARM é garantir e facilitar o acesso a esses dados, assim, é preciso encontrar um modelo adequado para representar as características informacionais e temporais dos dados climáticos coletados em uma base de dados, garantindo velocidades de armazenamento e consultas que atendam às necessidades dos usuários.

Nos testes realizados no estudo de caso descrito, empregaram-se três diferentes estratégias de ingestão de dados no Cassandra: Pandas, Batch e CSV; e duas estratégias de modelagem foram utilizadas. A primeira, adotou-se uma forma tabular um pouco mais complexa, em que todas as variáveis estão agregadas em uma mesma tabela multidimensional (wide-column strategy). Nesse caso, as variáveis bidimensionais são representadas pelo tipo de dado MAP do Cassandra, que mapeia para cada intervalo de coleta 680 ranges e seus respectivos valores. Na segunda estratégia de modelagem (single table strategy), procurou-se simplificar o modelo separando as variáveis unidimensionais e bidimensionais em diferentes tabelas. Nesse cenário, a dimensão de range ficou representada como um conjunto de colunas dentro da base de dados, gerando uma família de colunas que utiliza um amplo mapa multidimensional para armazenar os dados. O gráfico mostrado na Figura 2 apresenta os resultados sobre o desempenho na ingestão de dados do Cassandra das três estratégias nos dois cenários apresentados.

Figura I. TEMPO DE INSERÇÃO (MINUTOS)



A partir do Gráfico (Figura 2) pode-se concluir que a estratégia que utiliza uma única tabela é mais eficiente na inserção dos dados no Cassandra. Comparando as três estratégias utilizadas com a estratégia de uma única tabela, o CSV apresentou a maior velocidade de inserção, com 44 minutos, comparados aos 50 e 53 minutos do Batch e Pandas, respectivamente. Isso confirma a hipótese estabelecida de que os dados prontos em um arquivo CSV são importados mais rapidamente para dentro do Cassandra. O Batch, por ser um comando interno do CQL do Cassandra, também tem um melhor desempenho do que a carga de dados feita a partir do Pandas. No entanto, o CSV apresenta uma desvantagem importante com relação aos outros dois métodos, após a extração dos dados do arquivo NetCDF, esses dados precisam ser gravados em CSV em disco para que possa ser importado pelo Cassandra. Essa operação adiciona mais 5 minutos ao tempo de operação. Além disso, esse tempo para escrever os dados em CSV no disco, e de ler o arquivo CSV do disco para a tabela do Cassandra sobrecarrega o sistema. Assim, embora a inserção do CSV seja rápida, a sobrecarga na infraestrutura com gravações e leituras em disco torna essa estratégia desinteressante. Com relação à estratégia de *wide-column*, que separa as variáveis de acordo com suas dimensões, o Pandas obteve o melhor desempenho com 94 minutos. Nota-se que em todas as estratégias, o tempo de inserção dos dados foi muito maior se comparado à estratégia de tabela simples. Pode-se levantar dois motivos para esse fato. O primeiro é o fato de que a gravação de duas tabelas deve ocorrer em duas partições diferentes. O segundo fato é que a quantidade de células para inserções agora é muito maior. Se na estratégia de tabela simples o dados bidimensionais estavam alocados em um tipo de dados MAP, que armazena os dados como um vetor de JSON (JavaScript Object Notation) de literais, na estratégia *wide-column*, cada range das chaves do JSON torna-se uma coluna,

e os valores tornam-se registros do tipo *Float*, que é mais 'pesado' para carregar no banco de dados.

Outro ponto para comparação das estratégias foi verificar quais das duas estratégias de modelagem oferecia as consultas mais rápidas e eficientes. Nesse quesito, a estratégia *wide-column* apresentou uma vantagem significativa. A vantagem dessa estratégia está no nível conceitual de como funciona a modelagem no Cassandra. A implementação do código em Python ajudou a garantir que ambas as estratégias cumprissem os requisitos de consulta estabelecidos para a aplicação. Considerando a requisição de dados dentro de um range específico, o Cassandra possui uma limitação importante que é a incapacidade de retornar *subsets* de dados de uma linha de registro. Isso significa que para os dados requisitados para uma determinada data e horário, só seria possível retornar todos valores de ranges. Quer dizer que se usuário fizesse a requisição de dados dos 10 primeiros ranges, todos os 680 ranges seriam retornados pelo banco de dados, e os 670 ranges não requisitados seriam descartados pelo código em Python, mas a sobrecarga na consulta do banco de dados seria inevitável. A estratégia de *wide-column*, no entanto, seria capaz de lidar com esse tipo de situação com muito mais facilidade, uma vez que o código em Python determinaria as colunas do ranges requisitados e somente aqueles ranges seriam solicitados do banco de dados, evitando a sobrecarga de requisição de dados que não seriam usados.

Com relação à inserção, o *wide-column* foi mais lento que a estratégia de tabela simples, mas aqui vale mencionar algumas regras de negócio que validam o *wide-column* como mais apropriado. O tempo de inserção para cada arquivo pode ser considerado adequado porque em um dia de coleta, 23.385 amostragens são feitas em 24 horas, e levam 'apenas' 1 hora e 34 minutos para serem gravados no banco de dados.

Portanto, a estratégia de *wide-column* se mostrou mais adequada para o caso de estudo considerado. A modelagem da segunda dimensão dos dados bidimensionais como colunas mostrou-se mais adequada para consulta de dados, não causando um desperdício de recursos nas consultas e com tempo de inserção que satisfaz as necessidades do ARM.

IV. CONCLUSÃO

Este trabalho mostrou, por meio de um estudo de caso, como o modelo de dados e as estratégias de gravação afetam o desempenho de um banco de dados não-relacional no armazenamento e leitura de dados. Os dados considerados foram dados climáticos bidimensionais do ARM, e constatou-se que para inserção de dados, a estratégia de tabela *wide-column* apresenta desempenho pior se comparado à tabela simples, mas ganha em eficiência com relação à consulta aos dados. Finalmente, como trabalho futuro pretende-se explorar outras tecnologias de armazenamento de dados e incluir bancos de dados dedicados a séries temporais como *InfluxDB* e *TimescaleDB*, para fazer uma comparação de desempenho com os resultados do Cassandra.

ACKNOWLEDGMENT

This research was supported in part by an appointment to the Oak Ridge National Laboratory ASTRO Program, sponsored by the U.S. Department of Energy and administered by the Oak Ridge Institute for Science and Education.

REFERÊNCIAS

[1] PRIESS, Joerg A. et al. New EU-scale environmental scenarios until 2050 – Scenario process and initial scenario applications. Ecosystem Services, [s.l.], v. 29, p.542-551, fev. 2018. Elsevier BV. http://dx.doi.org/10.1016/j.ecoser.2017.08.006. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2212041617300232>. Acesso em: 25 set. 2018.

[2] National Oceanic and Atmospheric Administration (Org.). Climate Models. Disponível em: <https://www.climate.gov/maps-data/primer/climate-models>. Acesso em: 25 set. 2018.

[3] PEREIRA, Joana Castro. Environmental issues and international relations, a new global (dis)order - the role of International Relations in promoting a concerted international system. Revista Brasileira de Política Internacional, [s.l.], v. 58, n. 1, p.191-209, jun. 2015. FapUNIFESP (SciELO).. Disponível em: <http://dx.doi.org/10.1590/0034-7329201500110>. Acesso em: 28 set. 2018.

[4] CECCATO, Pietro; DINKU, Tufa. Introduction to Remote Sensing for Monitoring Rainfall, Temperature,Vegetation and Water Bodies. 2014. Disponível em: <https://iri.columbia.edu/~pceccato/Remote_Sensing_Introduction/Introduction_to_remote-sensing-environmental_monitoring.pdf>. Acesso em: 29 set. 2018.

[5] MCSWEENEY, Robert; HAUSFATHER, Zeke. How do climate models work? 2018. Disponível em: <https://www.carbonbrief.org/qa-how-do-climate-models-work>. Acesso em: 30 set. 2018.

[6] DATASAX (Org.). CQL shell commands. 2018. Disponível em: <https://docs.datastax.com/en/cql/3.3/cql/cql_reference/cqlshCopy.html>. Acesso em: 30 set. 2018.

[7] ARM. ARM'S Uniquely Continuous Climate Observations. Disponível em: <https://www.arm.gov/about/history>. Acesso em: 20 set. 2018.

[8] YOUNUS, Md Aboul Fazal. Research Methodology. Springer Theses, [s.l.], p.35-76, 2014. Springer Netherlands. Disponível em: <https://bit.ly/2OdrHap>. Acesso em: 02 out. 2018.

[9] SHUTTLEWORTH, Martyn. Case Study Research Design. 2008. Disponível em: <https://explorable.com/case-study-research-design>. Acesso em: 02 out. 2018.

[10] ARM. SOUTHERN GREAT PLAINS. Disponível em: <https://www.arm.gov/capabilities/observatories/sgp>. Acesso em: 01 out. 2018.

[11] Uddameri, Venki. (2017). Using R to read NetCDF Files. 10.17605/OSF.IO/8XCHE.

[12] CHEBOTKO, Artem; KASHLEV, Andrey; LU, Shiyong. A Big Data Modeling Methodology for Apache Cassandra. 2015 Ieee International Congress On Big Data, [s.l.], p.238-245, jun. 2015. IEEE. http://dx.doi.org/10.1109/bigdatacongress.2015.41. Disponível em: <https://ieeexplore.ieee.org/document/7207225?reload=true>. Acesso em: 03 out. 2018.

[13] Qiao, Jialin et al. "Heterogeneous Replica for Query on Cassandra." [astro-ph/0005112] A Determination of the Hubble Constant from Cepheid Distances and a Model of the Local Peculiar Velocity Field. October 02, 2018. Accessed October 04, 2018. https://arxiv.org/abs/1810.01037v1.

[14] MCKINNEY, Wes. Pandas: a Foundational Python Library for Data Analysis and Statistics. 2011. Disponível em: <https://www.researchgate.net/publication/265194455_pandas_a_Foundational_Python_Library_for_Data_Analysis_and_Statistics>. Acesso em: 04 out. 2018.

Machine Learning Interpretability applied to Autonomous Vehicles Safety

SILVA, A.R.*; Camargo, J.B.* (Alexandre Ray da Silva; João Batista Camargo Júnior)
*Safety Analysis Group, School of Engineering, University of São Paulo, São Paulo, Brazil
E-mail: alexandre.ray.silva@usp.br, joaocamargo@usp.br

***Abstract*—Deep Learning techniques have been widely used in a number of applications, among them the use in image recognition. Despite the promising results that these models have presented in recent years, there are still many doubts regarding the path that the algorithm goes through to make a decision, that is, one does not know how to explain how the model makes decisions. Thus, systems that are considered critical, such as those found in the health, finance, and transportation sectors, are becoming resistant to the use of such techniques, even knowing their potential benefit and performance. Many papers have been tried to minimize this problem and ensure clarity of the Deep Learning models. Methods such as LIME and SHAP have been created for example. This research consists of exploring this problem of interpretability in the context of autonomous vehicles. The purpose of this work is to design a neural network that will be able to recognize objects found in traffic (eg, pedestrians, boards, etc.) and to use interpretability tools to understand and propose improvements that the use of these techniques can bring to the safety and reliability of autonomous vehicles.**

***Keywords*— autonomous vehicle; safety-critical systems; machine learning; machine learning interpretability**

***Classification*— Master's degree**

***Category*— Beginner**

I. Introduction

Critical safety systems have the potential to produce catastrophic consequences to society, such as deaths, injuries, environmental and material damage. However, transportation systems, power generation, petrochemicals and a number of other critical safety systems are fundamental to the existence of society. In this way, developing and ensuring that critical systems are safe throughout their life cycle is a mission of engineering, science, and technology. Currently, given the state-of-the-art of systems technologies and paradigms, a framework of standards, regulations, techniques, disciplines and good practices can be considered to guarantee levels of safety considered adequate for systems in several areas of critical application, such as trains, chemical industry, aviation, etc. [1]. However, the recent and increasing introduction of new technologies and paradigms are transforming the current safety approaches. These approaches are becoming obsolete when dealing with critical systems. Among them, we can highlight the massive and pervasive use of advanced levels of Artificial Intelligence (eg, machine learning) both in planning (strategic level, development, support to tactical decision making) and in the operation and control of critical systems.

Some of the applications of Artificial Intelligence (AI) that gain more notoriety nowadays concern the autonomous vehicles. The tendency of the automobile industry is to move towards the development of autonomous vehicles. This is due to a number of factors such as safety improvements, increased productivity, decreased dependence on fuels and reduced congestion [2] [3] [4]. Autonomous vehicles are those where drivers are eliminated or have limited control over the vehicle due to the involvement of technologies such as sensors, cameras, communication systems and real-time data binding in the vicinity of the vehicle [5].

Recently, Deep Learning has quickly shaped the AI scenario [6]. This technique is being applied in many different areas, including image recognition, audio analysis and so on. Deep Learning and especially Convolutional Neural Networks represent an advance in the field of image analysis and computational vision [7]. In the context of autonomous vehicles, the use of sensors such as LIDAR and GPS, and calibrating them with cameras, it is possible to create an annotated dataset with location and relative speed. When generating a dataset with these markings, one can train a model of Deep Learning which is able to identify tracks, vehicles, pedestrians, etc. [8].

Safety applications for autonomous vehicles are essential prerequisites for the realization of an intelligent transportation system [9]. Among the components considered critical and that involve the detection of objects in images captured by the sensors of the autonomous vehicles, the following stand out:

- Detection of other vehicles — The vehicle detects and estimates the shape, size and all 3-dimensional locations in the vicinity of the vehicle;
- Road detection — Identify the steerable part of a street and its edges;
- Track Detection — Crucial for track swapping and fairly sensitive to safety;
- Pedestrian detection — Detection of people close to the streets. It has a great potential to avoid accidents;
- Drowsiness detection — Driver monitoring in order to take action before any accident occurs;
- Collision Avoidance — This is one of the key aspects of critical safety in autonomous vehicles. Collision avoidance systems help prevent accidents through automatic actions such as braking, turning, changing lanes, etc.

All previously presented items are considered critical in the context of autonomous vehicles. In other words, in the event of an erroneous or inaccurate detection, the autonomous system can cause accidents such as collisions between vehicles,

collisions in objects or even deaths.

Understanding why the model provides a certain prediction can be as crucial as the model's own accuracy in many applications. However, the highest accuracy is often achieved by a model that even the experts can not understand step by step prediction [10]. Given this, techniques to interpret and understand what a model learns have been used to make the validation process more robust [11]. Interpretability is especially important for autonomous vehicles, where model reliability must be guaranteed as it is a critical application and a failure can lead to an accident. It is noteworthy that in the scientific literature there are many works of image recognition in autonomous vehicles with the use of Deep Learning and there are many works that aim to explore the context of the interpretability of the models. However, there are few papers that explore the two contexts simultaneously.

The goal of this research project is to identify how the interpretive methods of Deep Learning used in the recognition of traffic images (eg, pedestrians, traffic lights, road signs, etc.) can contribute to the autonomous vehicles safety.

II. Methods

This section describes the main steps to follow in order to achieve the proposed goal on schedule. Initially, to reach the proposed objectives, a bibliographical review will be carried out, as well as a systematic review of the literature on the subject of the research in order to understand the state of the art of the problem. The next steps should be divided into three main strands:

A. Implementation and training of a deep neural network (DNN) which will be used to recognize images (eg, pedestrians)

At this phase of the project, a neural network capable of identifying pedestrians will be built. For training and testing of this model, it will be used the *"BDD100K: A Large-scale Diverse Driving Video Database" dataset* [12] from BAIR *(Berkeley Artificial Intelligence Research)*[1]. This dataset is one of the largest and most diverse driving video dataset. It is composed of videos of cars moving in the traffic.

The dataset is annotated and it has 100,000 videos. Each video is approximately 40 seconds long, 720p and 30 fps. The videos were collected in several places in the United States.

The base covers various weather conditions such as sunny, cloudy and rainy. The figure 1 shows the number of occurrences per object.

The tools used to implement the model will be the following: Python™ programming language, as well as tools that are inserted into the language ecosystem, such as NumPy, Sci-Py, TensorFlow, etc.

B. Application of interpretability techniques

After having a neural network trained and able to recognize pedestrians images in videos, I will enter a phase of exploratory analysis of this model by means of interpretive techniques. Among them, it will be used the following: SHAP [10] and LIME [13]. Both techniques have implementations whose source codes are readily available on the Github platform[2] [3]. In addition, both are agnostic to the model, that is, they are able to interpret any machine learning model. The following is a brief description of each:

1) **SHAP:** SHAPley (SHapley Additive exPlanations) is a unified framework for interpreting predictions. SHAP assigns each *feature* an importance value for a particular prediction. The SHAP introduces the idea that the explanation of a predictor model is also a model, called the explanation model.
2) **LIME:** The LIME proposes explanations for individual predictions for any classification or regression problem through local approximations with an interpretable model.

Fig. 1. Count for different types of objects. Source: [12]

C. Analysis

This stage consists of analyzing the results obtained from the application of SHAP and LIME interpretability techniques. In addition, it will be explored how these results influence the safety of the autonomous vehicles. That is, it must be identified how aspects of safety engineering such as reliability, availability, safety, and dependability can best be understood in the context of critical systems which uses Artificial Intelligence.

III. Expected Results

After the conclusion of this project, it is expected that the scientific community will have a robust and quality material which should contribute to the work of other researchers working in the areas of autonomous vehicles and interpretable machine learning. Also, it is expected that new *insights* should be generated from the model's explanations.

The results generated throughout this research project will be consolidated in the form of articles to be submitted to relevant conferences and newspapers of the area, whose theme is related to interpretable artificial intelligence or interpreting machine learning and critical safety in autonomous vehicles. In addition, the results will be disseminated to both the scientific community and the general public through lectures inside and outside the Polytechnic School School of Engineering of the University of São Paulo.

[1] https://bair.berkeley.edu/blog/2018/05/30/bdd/

[2] https://github.com/slundberg/shap

[3] https://github.com/marcotcr/lime

ACKNOWLEDGMENT

The authors would like to thank our colleagues from Safety Analysis Group from Escola Politécnica of Universidade de São Paulo who provided insight and expertise that greatly assisted this initial phase of the research.

REFERENCES

[1] P. Koopman and M. Wagner, "Autonomous Vehicle Safety: An Interdisciplinary Challenge," *IEEE Intelligent Transportation Systems Magazine*, vol. 9, no. 1, pp. 90–96, 2017.

[2] S. Duffy and J. Hopkins, "Sit, Stay, Drive: The Future of Autonomous Car Liability," 2013.

[3] W. Kumfer and R. Burgess, "Investigation into the Role of Rational Ethics in Crashes of Automated Vehicles," *Transportation Research Record: Journal of the Transportation Research Board*, vol. 2489, pp. 130–136, jan 2015.

[4] S. Urooj, I. Feroz, and N. Ahmad, "Systematic literature review on user interfaces of autonomous cars: Liabilities and responsibilities," in *2018 International Conference on Advancements in Computational Sciences (ICACS)*, pp. 1–10, IEEE, feb 2018.

[5] P.-L. Blyth, M. N. Mladenovic, B. A. Nardi, N. M. Su, and H. R. Ekbia, "Driving the self-driving vehicle: Expanding the technological design horizon," in *2015 IEEE International Symposium on Technology and Society (ISTAS)*, pp. 1–6, IEEE, nov 2015.

[6] J. Donahue, Y. Jia, O. Vinyals, J. Hoffman, N. Zhang, E. Tzeng, and T. Darrell, "DeCAF: A Deep Convolutional Activation Feature for Generic Visual Recognition," oct 2013.

[7] Hailong Li, Zhendong Wu, and Jianwu Zhang, "Pedestrian detection based on deep learning model," in *2016 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, pp. 796–800, IEEE, oct 2016.

[8] B. Huval, T. Wang, S. Tandon, J. Kiske, W. Song, J. Pazhayampallil, M. Andriluka, P. Rajpurkar, T. Migimatsu, R. Cheng-Yue, F. Mujica, A. Coates, and A. Y. Ng, "An Empirical Evaluation of Deep Learning on Highway Driving," apr 2015.

[9] C. Bila, F. Sivrikaya, M. A. Khan, and S. Albayrak, "Vehicles of the Future: A Survey of Research on Safety Issues," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, pp. 1046–1065, may 2017.

[10] S. Lundberg and S.-I. Lee, "A Unified Approach to Interpreting Model Predictions," may 2017.

[11] G. Montavon, W. Samek, and K.-R. Müller, "Methods for interpreting and understanding deep neural networks," *Digital Signal Processing*, vol. 73, pp. 1–15, feb 2018.

[12] F. Yu, W. Xian, Y. Chen, F. Liu, M. Liao, V. Madhavan, and T. Darrell, "BDD100K: A Diverse Driving Video Database with Scalable Annotation Tooling," may 2018.

[13] M. T. Ribeiro, S. Singh, and C. Guestrin, ""Why Should I Trust You?": Explaining the Predictions of Any Classifier," feb 2016.

A multiagent system for predicting customer demands
Um sistema multiagente para a predição de demandas de clientes

DONÂNCIO, H.*; BRANDÃO, A.*; (Henrique Donâncio Nunes Rodrigues; Anarosa Alves Franco Brandão)
*Laboratory of Intelligent Techniques - Escola Politécnica da USP
E-mail: donancio@ime.usp.br, anarosa.brandao@usp.br

***Abstract*—Agents are autonomous software components that can be combined in multiagent systems (MAS) and used to solve different problems. In this context, we present a proposal of MAS to predict customer demands of an electric energy distributor, analyzing the available tools for the construction of such systems. This system should be the basis for the definition of a scalable architecture to deploy MASaaS (Multiagent Systems as a Service).**

***Keywords*— Multiagent Systems; Smart Agents.**

***Resumo*— Agentes são componentes de *software* autônomos que podem ser combinados em sistemas multiagente (SMA) e usados para resolver diferentes problemas. Neste contexto, apresenta-se uma proposta de SMA para predição de demandas de clientes de uma distribuidora de energia elétrica, a partir da análise de ferramentas disponíveis para construção de tais sistemas. Este sistema deve ser a base para a definição de uma arquitetura escalável para implantar o MASaaS (Multiagent Systems as a Service).**

***Palavras-chave*— Sistemas Multiagente; Agentes Inteligentes.**

***Classificação*— Mestrado**

***Categoria*— Iniciante**

I. Introdução

Agentes podem ser descritos como entidades relativamente independentes e autônomas que podem ser usadas para resolver problemas de diferentes graus de complexidade [1]. Essas entidades podem ser organizadas em comunidades e trabalhar em conjunto usando diferentes mecanismos de interação para resolver problemas complexos. Tais comunidades também são conhecidas como sistemas multiagente (SMA): um sistema composto por múltiplos agentes que interagem entre si [2].

Devido às suas capacidades autônomas e interativas, os agentes podem ser vistos como um paradigma para a engenharia de *software*. Como as arquiteturas de *software* podem conter muitos componentes diferentes, cada um com seu próprio *thread* de controle e atribuições, os agentes podem ser usados como paradigma ao projetar tais sistemas [3]. Além disso, tal paradigma pode ser adotado em sistemas complexos, uma vez que a interação é uma das características mais importantes da complexidade do *software*.

Os agentes também são capazes de interagir com outros agentes, trocando dados e participando de interações complexas, como cooperação, coordenação e negociação. O principal objetivo de um SMA é resolver autonomamente problemas complexos que seriam impossíveis (ou muito difíceis) de resolver usando um sistema monolítico [3].

Agentes inteligentes são capazes de raciocinar e decidir qual ação executar de acordo com as informações disponíveis. Esta informação geralmente está relacionada às condições ou consequências das ações a serem executadas [3]. Aproveitar as capacidades inerentes aos agentes permite que o SMA se adapte às mudanças no ambiente. Além disso, o uso de múltiplos agentes permite que mecanismos de cooperação ocorram em situações em que a solução do problema em questão está além das capacidades de qualquer agente único. Aplicações de SMA incluem controle de manufatura, planejamento de produção, logística, transporte, entre outros [4].

Nesse contexto, ferramentas para o apoio de desenvolvimento de SMA são analisadas visando a construção de sistemas para atuação em larga escala, tendo como estudo de caso o atendimento e predição de demandas de clientes de uma distribuidora de energia elétrica. Nesse cenário, os agentes atuam a partir de informações decorrentes do padrão de comportamento dos usuários, baseado nos dados coletados pelo próprio sistema. Exemplos disso são: quando há maior requisição de segunda via de faturas e quais usuários costumam requisitá-la; alerta de vencimentos próximos; e soluções de atendimento em geral. Além disso, fatores ambientais, como risco de interrupção de fornecimento por avarias técnicas e eventual manutenção da rede próxima ao usuário.

Diante da natureza do problema em entender quando o usuário poderá requisitar informações e antecipá-las, um sistema multiagente autônomo mostra-se uma solução promissora dada suas capacidades inerentes de coordenação, tomada de decisões e aprendizado. Além disso, existem arcabouços para apoiar sua construção bem conhecidos na literatura [5] [6] [7].

Esse artigo está organizado da seguinte forma: na Seção II é apresentada algumas definições sobre agentes. Na Seção III alguns dos arcabouços disponíveis para construção de SMA são apresentados e na Seção IV esses arcabouços são comparados. Na Seção V, o estudo de caso de uma distribuidora de energia elétrica é brevemente discutido. Por fim, na Seção VI é apresentada uma conclusão.

II. Agentes Inteligentes

Não há consenso sobre a definição de agente, mas o elemento central que o define é a sua autonomia [3]. Em [8], [5] algumas características sobre agentes situados em algum *ambiente (mundo físico ou virtual)* são apresentadas:

- **Autonomia**: A autonomia nesse caso está relacionada a capacidade do agente em construir objetivos e tomar ações para que seja satisfeito, mesmo que isso em algum momento foi deliberado pelo sistema que ele *habita*, ou pela interação com outro(s) agente(s) ou humano(s).
- **Proatividade**: Proatividade significa ser capaz de exibir um comportamento dirigido a metas. Se um objetivo foi delegado a um agente, então espera-se que o agente tome ações para tentar alcançar este objetivo. Isso é diferente, por exemplo, de objetos em JAVA que são passivos, ou seja, somente apresentam um comportamento quando são invocados.
- **Reatividade**: A reatividade está relacionada a ser capaz de oferecer respostas devido a mudanças/estímulos no ambiente. Um agente racional reativo é capaz de traçar planos a partir dessas mudanças/estímulos de forma a atingir seus objetivos.
- **Habilidade Social**: A habilidade social aqui não se trata somente de se comunicar através de *bytes* ou invocando métodos uns sobre outros. Num SMA, habilidade social se refere a capacidade de comunicação entre os agentes possibilitando a troca de conhecimentos com o objetivo de compartilhar suas crenças e objetivos[1]. Também considera-se habilidade social a capacidade de participar de interações mais complexas, como cooperação, coordenação e negociação [2].

Um SMA composto por agentes orientados por objetivos é intrinsecamente adaptável, considerando que seus agentes possuem Autonomia, Proatividade, Reatividade e Habilidades Sociais.

III. Arcabouços de Sistemas Multiagente

A fim de comparar os arcabouços para apoiar o desenvolvimento de SMA, nosso primeiro critério foi escolher quais possuem código aberto e são usados ativamente pela comunidade multiagente. Além disso, também consideramos os arcabouços usados recentemente no evento anual *Multiagent Programming Context* [2]. Por fim, analisamos quais arcabouços eram capazes de prover as ferramentas adequadas para o desenvolvimento do projeto para então selecionar os seguintes: JaCaMo[3], JADE[4] e SPADE[5].

[1]No contexto de agentes BDI
[2]https://multiagentcontest.org/
[3]http://jacamo.sourceforge.net
[4]http://jade.tilab.com/
[5]https://pypi.org/project/SPADE/

A. JaCaMo

O arcabouço para programação de sistemas multiagente é constituído de três ferramentas: Jason [5], CArtAgO [9] e MOISE+ [10]), além da linguagem de programação de agentes AgentSpeak(L) [11].

1) Jason e a linguagem AgentSpeak(L): A plataforma Jason [5] é um interpretador de uma extensão da linguagem AgentSpeak, conhecida como AgentSpeak(L), baseada na arquitetura BDI (*Believes, Desires, Intentions*) [3]. Jason foi construído de forma a direcionar o comportamento do agente, sem que o programador tenha de se preocupar com isso.

A plataforma Jason é baseada na arquitetura BDI, portanto as crenças no Jason tem a função de representação do conhecimento. Um agente nessa arquitetura está constantemente percebendo o ambiente, alterando sua base de conhecimento, raciocinando sobre como agir de modo a atingir seus objetivos, e em seguida, agindo de modo a mudar o ambiente. A parte de raciocínio (prático) do comportamento cíclico do agente na linguagem AgentSpeak é feita de acordo com os planos que o agente tem em sua biblioteca de planos.

Um agente em AgentSpeak tem uma base de crenças, que expressam propriedades que o agente acredita serem verdadeiras do mundo em que está situado. Os objetivos expressam as propriedades dos estados do mundo que o agente deseja alcançar. Embora isso não seja imposto pela linguagem AgentSpeak, normalmente, ao representar um objetivo g em um programa de agente, significa que o agente está comprometido a agir de modo a mudar o mundo para um estado no qual g se torne realmente verdade [5]. A terceira construção essencial de um programa de um agente seguindo a arquitetura BDI são os planos, que ditam como um objetivo deve ser satisfeito. Alterações em crenças e em objetivos desencadeiam esses planos.

2) CArtAgO: O arcabouço CArtAgO (Common ARTifact infrastructure for AGents Open environments) [9] é baseado em agentes e artefatos (A & A) para modelar e projetar sistemas multiagente. Com esta ferramenta, pode-se criar artefatos estruturados em espaços abertos onde os agentes podem se unir para trabalhar em conjunto. Os artefatos são recursos e ferramentas, construídos dinamicamente, manipulados e usados por agentes para apoiar/realizar suas atividades individuais e coletivas.

Os principais elementos utilizados no CArtAgO são as propriedades observáveis, operações e sinais. Propriedades observáveis são elementos do artefato que o agente passa a observar de forma que qualquer operação sobre esse elemento será percebida. As operações são implementadas para fornecer uma interface para utilização dos recursos do artefato pelos agentes, com parâmetros de entrada e retorno *(OpFeedbackParam)*. Finalmente, os sinais *(Signals)* permitem que seja detectado pelo agente uma alteração em sua base de crenças, alterando-a. *Signals* podem ser úteis para desencadear ações a partir de artefatos, ou mesmo adicionar algo ao conjunto de *verdades* que o agente acredita.

3) MOISE+: O modelo organizacional MOISE+ [10] é uma ferramenta com intuito de modelar a organização de

um SMA. Consiste na especificação de três dimensões: a estrutural, onde são definidos papéis e ligações de heranças e grupos; a funcional, onde é estabelecido um conjunto de planos globais e missões para que as metas sejam atingidas; e a deôntica, que é a dimensão responsável pela definição de qual papel tem obrigação ou permissão para realizar cada missão.

B. JADE

O JADE (JAVA Agent Development Framework) é um *middleware* distribuído escrito em JAVA que requer um conhecimento mínimo sobre teoria de agentes para implementar agentes que são aderentes a FIPA[6]. O JADE usa o protocolo FIPA para comunicação, gerenciamento e arquitetura do agente.

Além de estabelecer as ações de comunicação compreendidas pelos agentes, o protocolo FIPA também especifica uma infra-estrutura de gerenciamento de agentes (chamada *Agent Platform*) e uma plataforma de publicação de serviços (denominada *Directory Facilitator*). O uso do JADE permite a identificação de todos os agentes através do uso de um identificador único (AID) em um ambiente distribuído. O *Directory Facilitator*, por outro lado, permite que os agentes publiquem serviços visíveis para outros agentes.

C. SPADE

SPADE (Smart Python multi-Agent Development Environment) é uma estrutura de agente escrita em Python e aderente a FIPA. A arquitetura BDI usada pelo SPADE é baseada em um esquema distribuído: todos os planos usados pelos agentes são representados na forma de serviços. Portanto, em vez de possuir uma biblioteca com vários planos, as ações dos agentes são definidas pelos serviços publicados no *Directory Facilitator*. Nesse sentido, um plano se torna uma composição de serviços oferecidos que são acessados pelo agente para que ele possa atingir os objetivos com os quais se comprometeu.

Este arcabouço é promissor do ponto de vista do desenvolvimento de agentes para expor os serviços, devido a sua própria natureza. Além disso, não é difícil encontrar desenvolvedores qualificados em Python.

IV. Comparação dos Arcabouços Multiagente

A partir da análise individual dos arcabouços apresentados na Seção III, estabelecemos os critérios de comparação entre eles, tendo como objetivo selecionar o mais adequado para apoiar o desenvolvimento de um MASaaS. Por essa razão, nos concentramos em (i) protocolos de comunicação e características associadas; (ii) representação de organização; (iii) suporte à linguagem de conteúdo; e (iv) suporte a ontologias. Este último é especialmente importante, pois ontologias podem ser usadas para modelar e consumir conhecimento de uma maneira interoperável [12]. Os resultados da comparação podem ser encontrados na Tabela I:

Tabela I
Características: JaCaMo, JADE e SPADE

	JaCaMo	JADE	SPADE
BDI	✓		✓
Directory Facilitator (DF)		✓	✓
Agent Management System (AMS)		✓	✓
FIPA-ACL		✓	✓
KQML	✓		
Multiplataforma	✓	✓	✓
Representação explícita da organização	✓		
Suporte a linguagem de conteúdo		✓	✓
Manipulação/criação de ontologias		✓	

É importante notar que o JADE e o SPADE possuem múltiplos pontos em comum - especialmente considerando a aderência ao protocolo FIPA. JaCaMo, por outro lado, usa um protocolo de comunicação conhecido como KQML [13]. Além disso, não possui especificações equivalentes ao *Directory Facilitator* (DF) e ao *Agent Management System* (AMS). Embora essas especificações não sejam necessariamente obrigatórias para a integração de agentes e serviços, elas certamente são importantes em cenários que envolvem um grande número deles. O DF funciona como as páginas amarelas[7] para catalogação e listagem de todos os serviços que podem ser usados pelos agentes. O AMS, por outro lado, é crucial para o estudo da transferência de mensagens e do gerenciamento de processos dentro dos arcabouços de SMA.

V. Sistema de predição de demandas de clientes

O sistema de predição de demandas de clientes de uma distribuidora de energia elétrica que pretende-se implementar baseia-se em módulos de tarefas e seus respectivos agentes (ver Figura 1), que são: (i) atendimento, (ii) monitoramento de fornecimento e (iii) financeiro. A seguir são apresentados detalhes de cada um desses módulos, bem como um esboço do sistema que será criado.

O atendimento concentra-se em um canal de atendimento *online* onde o cliente acessa com sua respectiva matrícula cadastrada no sistema. Esse atendimento será feito através de um *chatbot*, que de maneira geral é um agente que utiliza Processamento de Linguagem Natural (PLN) [14] para interagir com o cliente. Um dos objetivos desse canal é o agrupamento de demandas. Esse agrupamento visa estabelecer um conjunto determinados clientes/solicitações de modo a antecipar informações. Por exemplo, se vários usuários de uma mesma região acessam o canal de atendimento questionando sobre a falta de fornecimento de energia, há grande possibilidade de que novos atendimentos iniciados dessa mesma região venham solicitar essas mesmas informações. Um dos objetivos desse sistema é predizer demandas desta natureza e satisfazê-las antes que o cliente tenha de solicitá-las.

O monitoramento de fornecimento é um processo interno do sistema de fornecimento de energia para monitorar sua operação. Eventuais falhas de serviço são comunicadas entre agentes desse sistema. JADE por exemplo, possui a capacidade de criação de agentes móveis, que podem ser embarcados em

[6]http://www.fipa.org/

[7]Páginas amarelas em catálogos de serviços de telefonia fixa

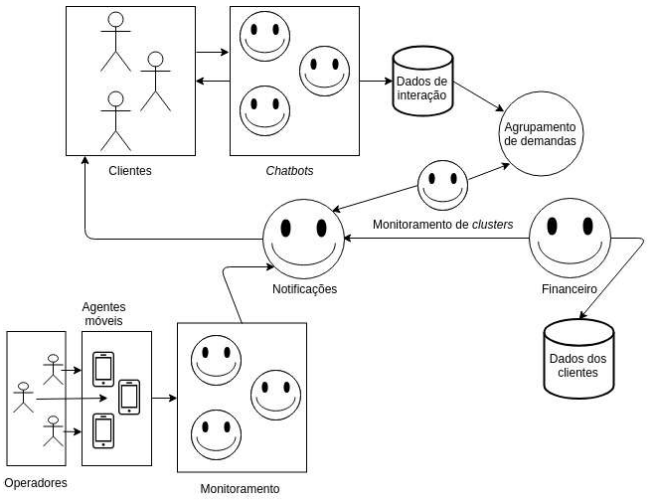


Figura 1. Sistema de predição de demandas

dispositivos transportados pela equipe de manutenção da rede. Desta forma é possível estimar o tempo de reparo e comunicá-lo a um agente responsável por distribuir essa informação para clientes da localidade onde o reparo será feito, evitando assim eventuais transtornos dado ao congestionamento de vias e a falta de serviço.

O módulo financeiro, de forma geral, analisa o comportamento do cliente e eventualmente encaminha segunda via de faturas antes que o cliente solicite. Os agentes responsáveis por essa tarefa estão constantemente verificando a base de dados para orientar suas ações.

Questões de escalabilidade estão intrínsecamente relacionadas ao número de clientes que acessam o sistema, bem como ao tamanho da equipe de manutenção e sua respectiva área de cobertura

VI. Conclusão

Esse artigo apresentou um esboço de SMA para predição de demandas de uma distribuidora de energia elétrica. Para definir qual ferramenta apoiaria o desenvolvimento do SMA foram avaliados três arcabouços: JaCaMo, JADE e SPADE. Uma análise comparativa sobre funcionalidades de interesse para apoiar o desenvolvimento de MASaaS foi apresentada, seguida da definição da arquitetura que o MASaaS deve possuir.

Em trabalhos futuros, pretende-se fazer um estudo das capacidades operacionais dos arcabouços, como por exemplo, o desempenho em sistemas de larga escala, bem como a complexidade de integração com outros sistemas. O objetivo é construir um sistema multiagente que consiga atender uma densidade alta de requisições simultâneas tendo como base o estudo de caso da distribuidora de energia elétrica. Posteriormente a essa fase, é necessário um estudo das principais ferramentas para PLN, e sua integração com a tecnologia voltada a agentes.

Agradecimentos

Este trabalho tem o apoio do programa de P&D ANEEL.

Referências

[1] FERBER, J. *Multi-agent systems: an introduction to distributed artificial intelligence*. [S.l.]: Addison-Wesley Reading, 1999. v. 1.

[2] RUSSELL, S. J.; NORVIG, P. *Artificial Intelligence: A Modern Approach*. 2. ed. [S.l.]: Pearson Education, 2003. ISBN 0137903952.

[3] WOOLDRIDGE, M. *An introduction to multiagent systems*. [S.l.]: John Wiley & Sons, 2009.

[4] PĚCHOUČEK, M.; MAŘÍK, V. Industrial deployment of multi-agent technologies: review and selected case studies. *Autonomous agents and multi-agent systems*, Springer, v. 17, n. 3, p. 397–431, 2008.

[5] BORDINI, R. H.; HÜBNER, J. F.; WOOLDRIDGE, M. *Programming multi-agent systems in AgentSpeak using Jason*. [S.l.]: John Wiley & Sons, 2007. v. 8.

[6] GREGORI, M. E.; CÁMARA, J. P.; BADA, G. A. A jabber-based multi-agent system platform. In: ACM. *Proceedings of the fifth international joint conference on Autonomous agents and multiagent systems*. [S.l.], 2006. p. 1282–1284.

[7] BELLIFEMINE, F. L.; CAIRE, G.; GREENWOOD, D. *Developing multi-agent systems with JADE*. [S.l.]: John Wiley & Sons, 2007. v. 7.

[8] WOOLDRIDGE, M.; JENNINGS, N. R. Intelligent agents: Theory and practice. *Knowledge Engineering Review*, v. 10, p. 115–152, 1995.

[9] RICCI, A.; VIROLI, M.; OMICINI, A. Cartago: A framework for prototyping artifact-based environments in mas. In: SPRINGER. *International Workshop on Environments for Multi-Agent Systems*. [S.l.], 2006. p. 67–86.

[10] HUBNER, J. F.; SICHMAN, J. S.; BOISSIER, O. Developing organised multiagent systems using the moise+ model: programming issues at the system and agent levels. *International Journal of Agent-Oriented Software Engineering*, Inderscience Publishers, v. 1, n. 3-4, p. 370–395, 2007.

[11] RAO, A. S. Agentspeak (l): Bdi agents speak out in a logical computable language. In: SPRINGER. *European Workshop on Modelling Autonomous Agents in a Multi-Agent World*. [S.l.], 1996. p. 42–55.

[12] BECHHOFER, S. Owl: Web ontology language. In: *Encyclopedia of database systems*. [S.l.]: Springer, 2009. p. 2008–2009.

[13] FININ, T. et al. Kqml as an agent communication language. In: *Proceedings of the Third International Conference on Information and Knowledge Management*. New York, NY, USA: ACM, 1994. (CIKM '94), p. 456–463. ISBN 0-89791-674-3. Disponível em: <http://doi.acm.org/10.1145/191246.191322>.

[14] INDURKHYA, N.; DAMERAU, F. J. *Handbook of natural language processing*. [S.l.]: CRC Press, 2010. v. 2.

Interpretability as an Auditing Tool: Generating Reports from Black-Box Classifiers
Interpretabilidade como Ferramenta de Auditoria: Geração de Relatórios a Partir de Classificadores Caixa-Preta

AQUINO, R. M.*; COZMAN, F. G.*
*Escola Politécnica da Universidade de São Paulo
E-mail: rodrigo-monteiro.aquino@usp.br, fgcozman@usp.br

***Abstract*—Recent legislation guarantees to every citizen the right of explanation for any given decision taken automatically by an autonomous system. Therefore, it is necessary that black-box classifiers, particularly the more complex ones (e.g. neural networks) have their decisions interpreted and explained, especially in cases where financial and banking decisions are involved. Several techniques have been developed to explain automatic decisions, but in general they focus only on learning a "simple" classifier that helps to understand the "complex" one. The objective of this project is to propose and implement techniques to automatically create reports that are in fact comprehensible by regulation entities, using "simple" classifiers as an intermediary step.**

***Keywords*— Interpretability; Machine Learning, Auditing.**

***Resumo*— Leis recentes garantem a todo cidadão o direito de receber explicações sobre decisões que o afetam e que sejam tomadas automaticamente. Em vista disso, é necessário que classificadores "caixa-preta", em geral de alta complexidade (por exemplo, redes neurais profundas), tenham suas decisões interpretadas e explicadas, em particular em casos que envolvem decisões e recomendações bancárias e financeiras. Diversas técnicas têm sido desenvolvidas para explicar decisões automáticas, mas em geral tais técnicas procuram aprender um classificador "simples" que serve como explicação para um classificador "complexo". O objetivo deste projeto é propor e implementar técnicas de geração automática de relatórios que sejam de fato compreensíveis por entidades reguladoras, usando classificadores "simples" como passo intermediário.**

***Palavras-chave*— Interpretabilidade; Aprendizado de Máquinas, Auditoria.**

***Classificação*— Mestrado**

***Categoria*— Iniciante**

I. Introdução e Motivação

A comunidade interessada em aprendizado de máquina tem dedicado esforços para desenvolver técnicas que permitam a interpretação de classificadores "caixa-preta" como por exemplo redes neurais profundas [1], [2]. Procura-se com isso aumentar a satisfação do usuário do classificador, além de melhorar o entendimento sobre o próprio classificador. Por exemplo, suponha que o classificador use uma *random forest* com 100 diferentes árvores de altura 10 para classificar clientes em "bons pagadores" e "maus pagadores". Uma vez que um cliente tem seu crédito negado com base na saída desse classificador, seria desejável fornecer ao cliente uma explicação curta e compreensível sobre a decisão. Por outro lado, se o classificador indica como "bom pagador" um cliente que é reconhecidamente mau pagador, o projetista do classificador pode se basear em uma explicação gerada pelo classificador para entender qual é a razão da classificação incorreta.

Além disso, existem questões legais que reforçam a necessidade de explicar decisões tomadas automaticamente por classificadores complexos. Em particular, a a regulação europeia *General Data Protection Regulation* (GDPR) [3] garante a um cidadão, entre outros pontos, o direito à explicação sobre uma decisão realizada por um sistema automatizado. No Brasil, o Projeto de Lei 4060/2012, que foi aprovado Congresso Nacional e sancionado pela presidência como Lei Ordinária nº 13.709/18, segue essa mesma tendência.

A preocupação com interpretabilidade em aprendizado de máquina se tornou mais aguda nos últimos anos, à medida que modelos mais complexos passaram a exibir excelente desempenho. Um importante acontecimento foi o lançamento, em 2016, de uma linha de financiamento pelo DARPA (*Defense Advanced Research Projects Agency*), órgão do governo norte-americano, em "*Explainable Artificial Intelligence*" [1]. Desde então, um grande número de projetos foi lançado ao redor do mundo, bem como vários encontros científicos no tema (por exemplo, a *International Joint Conference on Artificial Intelligence* de 2018 teve um conjunto de quatro *workshops* voltados a *Explainable AI*).

Frequentemente se entende uma atividade de aprendizado de máquina como um processo com várias etapas: pré-processamento e preparação dos dados; seleção de atributos; treinamento de modelo; teste do modelo; uso do modelo. O foco em interpretabilidade exige que o uso do modelo seja acompanhado de uma explicação do modelo. Caso o modelo já seja facilmente interpretável, a explicação pode ser

a apresentação do próprio modelo (por exemplo, se o modelo é um regressor logístico, o próprio regressor pode ser de fácil entendimento para um particular usuário). Caso o modelo não seja facilmente interpretável, a explicação precisa ser dele extraída. Duas estratégias têm sido usadas na literatura para produzir explicações para um classificador "complexo".

A primeira estratégia foca nas características do classificador "complexo", procurando traduzir seu comportamento interno de forma textual ou visual. Por exemplo, a decisão de uma rede neural profunda pode ser "explicada" indicando quais pesos na rede afetaram a decisão, e por conseguinte indicando quais partes da entrada afetaram a saída [4]. Esse tipo de explicação presume um usuário com conhecimento do modelo complexo.

Uma estratégia alternativa procura aprender um classificador "simples" a partir das entradas e saídas do classificador "complexo" [5], [6], [7], [8], [2]. Por exemplo, considere uma rede neural profunda que faz classificação de imagens, e um regressor logístico que aproxima o comportamento da rede: o regressor logístico serve então como interpretação da rede. Diz-se nesse caso que o método de interpretação é agnóstico ao modelo, pois apenas a entrada e saída do classificador "complexo" são usadas.

A fidelidade de um método agnóstico ao modelo mede o quão próximos estão o classificador "simples" e o classificador "complexo". Para garantir uma boa fidelidade, em geral usa-se apenas aproximações locais: ou seja, um classificador "simples" é gerado para cada particular decisão tomada pelo classificador "complexo" [2].

Ainda que um classificador "complexo" seja reduzido a um outro classificador "simples", resta a questão de como apresentar esse resultado para o usuário. Obviamente, essa apresentação depende do usuário: uma regressão logística pode ser óbvia para um usuário e complexa para outro.

O objetivo deste projeto é propor e implementar ferramentas que partam de um classificador "complexo" e, usando métodos agnósticos ao modelo, chegue em uma explicação textual e compreensível para efeito de auditoria do classificador "complexo" (ou seja, uma explicação que permita entender como o classificador "complexo" processou a entrada).

II. Relevância e Potenciais Aplicações

Resultados obtidos nesse projeto serão relevantes para todas as tarefas de classificação onde um usuário humano precisa receber explicações sobre decisões automáticas, e em particular quando um processo de auditoria é aplicado para verificar se explicações claras são de fato geradas.

Por exemplo, o arcabouço a ser desenvolvido será importante para apoiar recomendações sobre investimentos ou sobre crédito que sejam realizadas de forma automática e que devam ser comunicadas a clientes.

Mais especificamente, áreas de atuação que não se utilizam de modelos complexos devido à sua impossibilidade de interpretacão (requerida por órgãos reguladores), passarão a explorar os resultados de tais modelos. Tomando como exemplo o mercado de crédito, o qual instituições financeiras usam apenas modelo tradicionais pois são interpretáveis por natureza, a utilização de modelos no estado da arte impactaria um aumento na assertividade de decisões tomadas sem perder clareza do modelo.

III. Metodologia de Pesquisa

Em um primeiro momento, será realizada a avaliação de técnicas de interpretabilidade disponíveis na literatura, como as apresentadas pelos sistemas LIME [2], MAGIX [8], e ActiVis [9]. Tais sistemas são identificados na literatura como estado da arte no campo de interpretabilidade de modelos, e no escopo desta pesquisa serão aplicados a problemas de classificação publicamente disponíveis para que seu desempenho seja avaliado.

Em seguida, serão estudadas quais são as exigências de autoridades reguladoras de interesse no que diz respeito à interpretabilidade de decisões. O foco será mantido em decisões bancárias, como por exemplo recomendações de crédito. Será buscada uma interação com membros da área que tenham experiência no setor, para construir um panorama das exigências legais e práticas sobre sistemas de classificação automáticos.

O projeto será direcionado então ao estudo das tecnologias de geração de textos, área em grande evolução [10], [11] atualmente. Existem métodos baseados em *templates* e também em diferentes técnicas de processamento de linguagem natural, os quais são extensivamente explorados em [12] e embasados em [13]. No contexto desse projeto é importante produzir um texto de fácil entendimento e conciso, que permita capturar toda a explicação (fornecida pelo classificador "simples") de forma breve. Serão comparadas diversas técnicas e selecionadas as que melhor se adequam às necessidades do projeto.

Finalmente, as várias técnicas estudadas e testadas deverão ser selecionadas e combinadas em processo harmonioso. Um arcabouço completo será definido e implementado. Testes serão feitos com usuários humanos através da *Amazon Mechanical Turk* (esse é um procedimento comum para teste na literatura sobre interpretabilidade).

O *Amazon Mechanical Turk* é um serviço que se propõe a atender demandas de inteligência humana por meio de uma plataforma online. Este atendimento é acessivel pela interface digital (API - *Application Programming Interface*) da Amazon, permitindo a conexão de aplicativos a uma força de trabalho que atende tais demandas.

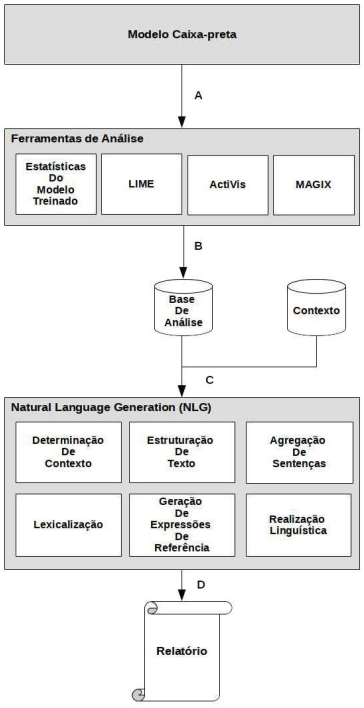
IV. Desenvolvimento

A estrutura preliminar do projeto, ilustrado pela Figura 1, representa a estratégia de análise de um modelo caixa-preta.

É importante ressaltar que o bloco caracterizado como *Natural Language Generation* está segmentado de acordo com [12], sendo que cada segmento será abordado e avaliado de maneira diferente para a obtenção de um texto adequado.

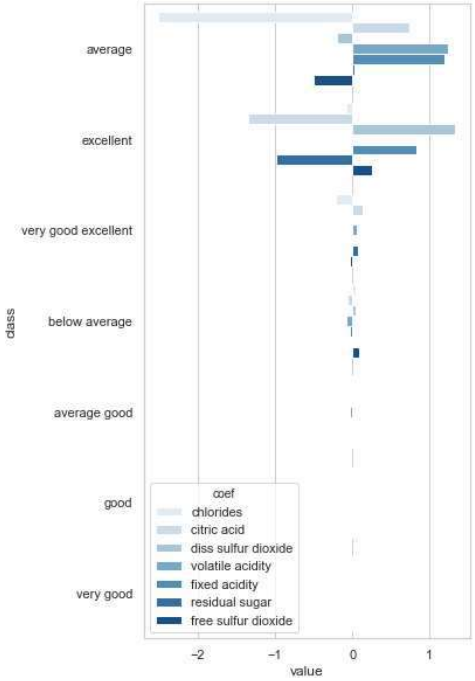
As transições representadas na figura são descritas a seguir:

Figura 1. Estrutura Preliminar



Fonte: Autor

Figura 2. Coeficientes do modelo disponível em [14]



Fonte: Autor

A. *Análise do Modelo*

Utilização de estatísticas expressas diretamente pelo modelo treinado e a partir de ferramentas de interpretabilidade apresentadas pela literatura para a extração de dados relevantes.

B. *Armazenamento de Dados*

Armazenamento estruturado dos dados extraídos, de forma a padronizar o *output* dos modelos analisados para manter a solução final agnóstica ao modelo analisado.

C. *Convergência de Dados*

Integração dos dados referentes ao contexto de interesse para a utilização conjunta com os dados extraídos do modelo.

D. *Geração de Relatório*

Aplicação de técnicas de geração de texto em linguagem natural (*Natural Language Generation* - NLG) para a geração de relatórios coesos e coerentes com o contexto, utilizando como insumo os dados resultantes das fases anteriores.

A fase atual de implementação desta estratégia encontra-se na análise das estatísticas expostas por um modelo treinado e exposição deles de maneira textual. A técnica utilizada para a criação de textos é de geração dinâmica de *templates*, de acordo com os dados apresentados é realizada uma análise comparativa diferente.

De acordo com o avanço do projeto serão implementadas técnicas mais avançadas de geração de texto, de acordo com o ilustrado pelo bloco *Natural Language Generation* da Figura 1.

V. Resultados Preliminares

A estrutura de análise proposta já se encontra em desenvolvimento, sendo que sua implementação inicial apresenta uma interpretação textual de um modelo regressão logística.

O modelo de regressão logística foi escolhido devido à percepção de que este é “interpretável”, no entanto quando a dimensionalidade do problema é alta aumenta-se a dificuldade de explicar tal modelo.

A interpretação gerada se apresenta por meio de um template dinamicamente construído, formatado e preenchido de acordo com os resultado da análise realizada nas informações obtidas a partir modelo treinado.

A Figura 2 apresenta os coeficientes de uma regressão logística que foi treinada com o uso da base de dados originária de [14], referente à qualidade de vinhos baseado em suas propriedades físicas. Esta base possui 6.497 entradas, divididas em 1.599 exemplos de vinhos tintos e 4.898 de vinho branco com as seguintes propriedades: **fixed acidity**, **volatile acidity**, **citric acid**, **residual sugar**, **chlorides**, **free sulfur dioxide**, **diss sulfur dioxide**, **total sulfur dioxide**, **density**, **pH**, **sulphates**, **alcohol**, **type** e **quality**.

Apenas as colunas **diss sulfur dioxide** e **type** foram obtidas a partir de manipulação dos dados da base. A coluna **type** foi gerada para identificar se o vinho é tinto ou branco (as bases foram disponibilizadas em bases separadas), e **diss sulfur dioxide** é resultado da diferença entre **total sulfur dioxid** e **free sulfur dioxide**. As manipulações foram mínimas pois o foco final era a análise do modelo e não a otimização dele.

De posse destes coeficientes é possível realizar algumas análises para o preenchimento de um *template*, cujo exemplo pode ser observado no trecho abaixo destacado:

> Given the possible values that the model can predict ({{**list_values**}}), the classes {{**1st_top_class**}} and {{**2nd_top_class**}} were considered more relevant.

As lacunas a serem preenchidas são representadas pelos símbolos "{{" e "}}", que determinam os limites inicial e final de preenchimento. Os termos apresentados internamente,em negrito, são preenchidos com informações geradas a partir das análises realizadas nos dados do modelo, fase representada na Figura 1 como "Ferramentas de Análise". Eles são definidos como:

- **list_values**: nomes de classes possíveis;
- **1st_top_class**: nome da classe com o maior valor médio absoluto dos coeficientes da regressão logística;
- **2nd_top_class**: nome da classe com o segundo maior valor médio absoluto dos coeficientes da regressão logística.

O resultado obtido a partir da análise deste modelo e o preenchimento do template completo podem ser observados no trecho destacado:

> Given the possible values that the model can predict (**below average, average, average good, good, very good, very good excellent, excellent**), the classes **average** and **excellent** were considered more relevant. Analysing the prediction of **average**, the most relevant features that indicates a "true" prediction were: **volatile acidity** and **fixed acidity**. On the other hand, features **chlorides** and **free sulfur dioxide** contributed to a "false" prediction.
> Similarly, the class **excellent** was more represented by the features **diss sulfur dioxide** and **fixed acidity** to indicate a "true" prediction, and features **citric acid** and **residual sugar** contributed to a indicate a "false" prediction.

VI. Próximos Passos

Como visto na seção V, ainda são realizadas apenas análises básicas no modelo em estudo. Com o avanço do projeto, análises mais detalhadas serão implementadas por meio de ferramentas disponíveis na literatura (*e.g.* [2], [9], [8]). Com isso pretende-se aumentar o nível de detalhe na geração de dados analíticos, permitindo aumentar os insumos para a geração de informações relevantes.

Quanto à representação textual dos dados extraídos do modelo, o objetivo será o desenvolvimento de um sistema genérico para a geração dinâmica de sentenças (bloco ilustrado na Figura 1), baseando-se nos conceitos de *Natural Language Generation* por [13]. Esta implementação implicará na geração de textos mais naturais, no sentido de facilidade de leitura, e melhor gerenciáveis (comparativamente ao uso de *templates*).

VII. Resultados Esperados

O presente projeto desenvolverá técnicas que partem de classificadores caixa-preta e produzem relatórios explicativos que possam ser aceitos por entidades reguladoras. Tais relatórios serão textos estruturados expressos em linguagem natural, que possam ser usados para auditar classificadores caixa-preta e de fato comunicar seu funcionamento a entidades externas.

Agradecimentos

Este trabalho foi realizado com o apoio do Itaú Unibanco S.A., por meio do Programa de Bolsas Itaú (PBI), vinculado ao Centro de Ciência de Dados da Escola Politécnica da USP. O projeto também recebeu apoio financeiro da FAPESP (processo nº 2016/18841-0). O segundo autor é parcialmente apoiado pela CNPq (processo nº 308433/2014-9).

Referências

[1] DARPA-BAA-16-53. Explainable Artificial Intelligence (XAI). *Defense Advanced Research Projects Agency*, p. 1, 2016. Disponível em: <https://www.darpa.mil/program/explainable-artificial-intelligence>.

[2] RIBEIRO, M. T.; SINGH, S.; GUESTRIN, C. Nothing Else Matters: Model-Agnostic Explanations By Identifying Prediction Invariance. n. Nips, 2016. Disponível em: <http://arxiv.org/abs/1611.05817>.

[3] European Union. Regulation 2016/679 of the European parliament and the Council of the European Union. *Official Journal of the European Communities*, p. 1–88, 2016.

[4] ANDREWS, R.; DIEDERICH, J.; TICKLE, A. B. Survey and critique of techniques for extracting rules from trained artificial neural networks. *Knowledge-Based Systems*, 1995. ISSN 09507051.

[5] CHEN, J. et al. Learning to Explain: An Information-Theoretic Perspective on Model Interpretation. 2018. Disponível em: <http://arxiv.org/abs/1802.07814>.

[6] GUIDOTTI, R. et al. A Survey Of Methods For Explaining Black Box Models. feb 2018. Disponível em: <http://arxiv.org/abs/1802.01933>.

[7] HECHTLINGER, Y. Interpretation of Prediction Models Using the Input Gradient. n. Nips, 2016. Disponível em: <http://arxiv.org/abs/1611.07634>.

[8] PURI, N. et al. MAGIX: Model Agnostic Globally Interpretable Explanations. 2017. Disponível em: <http://arxiv.org/abs/1706.07160>.

[9] KAHNG, M. et al. ACTIVIS: Visual Exploration of Industry-Scale Deep Neural Network Models. *IEEE Transactions on Visualization and Computer Graphics*, p. 1–1, 2017. ISSN 1077-2626. Disponível em: <http://ieeexplore.ieee.org/document/8022871/>.

[10] GKATZIA, D.; LEMON, O.; RIESER, V. Data-to-Text Generation Improves Decision-Making Under Uncertainty. *IEEE Computational Intelligence Magazine*, 2017. ISSN 1556603X.

[11] PERERA, R.; NAND, P. Recent advances in natural language generation: A survey and classification of the empirical literature. *Computing and Informatics*, 2017.

[12] GATT, A.; KRAHMER, E. Survey of the state of the art in natural language generation: Core tasks, applications and evaluation. *Journal of Artificial Intelligence Research*, 2018. ISSN 10769757.

[13] REITER, E.; DALE, R. *Building natural language generation systems*. [S.l.]: Cambridge University Press, 2000. 248 p. ISBN 0521620368.

[14] CORTEZ, P. et al. Modeling wine preferences by data mining from physicochemical properties. *Decision Support Systems*, North-Holland, v. 47, n. 4, p. 547–553, nov 2009. ISSN 0167-9236. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167923609001377>.

Fault diagnosis to prevent wheels and bearings overheating in heavy haul railway operations

Oliveira, D. F. N.*; Almeida Junior, J.R.*
*Safety Analysis Group, School of Engineering, University of Sao Paulo, São Paulo
davidoliveira@usp.br, jorgerady@usp.br

***Abstract*— A common challenge in the maintenance processes lies on the mitigation of recurrent failures. The ability to diagnose root faults could optimize the operation availability and repair effectiveness. Condition-based maintenance (CBM) proposes the repair planning before the incident by predicting the remaining useful life (RUL) of the components. This approach is generally done through the state pattern recognition and mapping wear evolution along the time. However, applying prediction techniques with no proper fault diagnosis leads treating recurrent failures with palliative solutions, since the source fault is still unknown and the failure might manifest in a near future. The research proposes the evaluation and mixture of techniques to build a model able to identity latent faults related to overheating of rail car wheels and bearings, where it is observed to be the most frequent failure related to rail cars. The case study will base the research simulated measurements of temperature, vibration, acoustic and wheel geometry profile from heavy haul railways operations. As an initial result, this paper introduces about applied techniques in fault diagnosis, cause-effects of overheating over rolling stock pieces, describe the types of sensors used in measurements, partial results, outlooks and future steps for the research.**

Keywords*— *condition-based maintenance; fault diagnosis, rolling stock, wheel set, bearing
Classification*— *master degree
Category*— *beginner

I. INTRODUCTION

Adequate maintenance processes are a fundamental part to achieve operational efficiency providing higher availability, reliability and better usage of machinery considering performance and acceptable wear rate. Any deviations from the correct service are called failures and the possible causes are known as faults [7]. Regardless the maintenance type [1], fault analysis and diagnosis comprehend an important discipline to solve problems by focusing on root causes, enabling better decisions about maintenance planning and tasks. This approach can reduce recurrent incidents, which lead to several operational and financial disturbances: (i.) increasing of unnecessary service maintenance requests, (ii.) reduction of asset operations availability, (iii.) premature replacement of components by abnormal behaviors of a physical asset [5].

In the context of heavy haul transports, a railway line must support very intense traffics to reach the planned production. A failure could represent a complete stoppage of the line affecting all trains in subsequent transits. It is well discussed in literature that most of the corrective maintenance tasks come from overheating faults.

As the final objective, this research plans to explore machine learning and statistical methods to propose a robust fault diagnosis model capable to map the major cause-effects and predict faults that leads to overheating problems in heavy haul rail car. A systematic literature review is already in progress in order to identify current approaches, state-of-the-art and possible gaps that could be filled.

Section 2 present some related works applied to fault diagnosis. Section 3 gives a high level overview about the detrimental effects of overheating in rolling stock components. Section 4 introduces the type of sensors used for measurements. Section 5 concludes about of possible future steps in the research based on the current point of view.

II. RELATED WORKS

Many techniques from statistics, artificial intelligence (AI) and domain specific models have been applied to fault diagnosis, where can be categorized in model-based, data-driven and signal-based methods [22][23]. Model-based depends of knowledge from physical principles and system specification dependencies. High complex systems may be not adequate for model-based. Data-driven acts as a black box system, where for any input, the model delivers an output with no logical demonstration how it was reached. Besides the option can reach high accuracy, it must be combined other methods in order to describe causalities. Signal-driven treats the data sequentially, where it is largely applied in time series predictions. Any diagnose is done by prior states (pattern symptoms) and knowledge of possible trends. Some general techniques in diverse knowledge domains are:

- Exploratory data analysis (EDA) to obtain high order information [5] such as means, medians, skewness, kurtosis, counts, correlations, regressions and statistical hypothesis tests [16] like t tests, chi squared, ANOVA, analysis of similarities (ANOSIM) and others. EDA can bring useful insights by visualization plots.
- Time series analysis are largely used in fault detection [21]. However, many cases have combined with other methods in order to understand sequential states and classify faults, such as auto regressive moving average methods, Kalman filters [16], Wavelets and Fourier transforms [15], and many others [18][21].
- Fault tree analysis [8][19] and Petri nets [8] are applied in domain environments where relation of cause-effect are well known.

- Unsupervised learning to find similarities by grouping records through clustering techniques such as k-means, c-means and Gaussian Mixture Models (GMM) [25]. Dimensionality reduction methods could eliminate useless variables in the modeling, such Principal Component Analysis (PCA) [15][21], Fisher Discriminant Analysis (FDA) [20] and sparse autoenconders models for deep neural networks (DNN) approaches [26][27].
- Some types of artificial neural networks (ANN) applied with methods, such as Restricted Boltzmann Machines (RBM) [14], Multi Layer Perceptron (MLP) [15][22], Radial Basis Function (RBF) and Self Organizing Maps (SOM) [21]. Deep Neural Networks have been pointed as the state-of-the-art for some complex domains as speech recognition, machine vision and translation [30]. Some authors are also proposing as powerful models for fault diagnosis due to the great ability to learn and represent complex features through the use of deep convolutional neural networks (DCNN) [28] [29] autoencoders [26] [27]
- Probabilistic graph modeling (PGM) such as Bayesian Networks [3][4][17], Hidden Markov Models [14] and RBM (already introduced as ANN option) have bee cited as modern and powerful approaches in risk analysis in order to identify reproduce structures of non deterministic dependencies between variables.

III. Overheating cause-effects over rolling stock components

As already presented, overheating has been the most recurrent problem reported by the maintenance team in the case study. Wheel temperature is mainly affected by vehicle speed, dissipated power and contact patch size by rail-wheels geometry state [10]. Failures in traction control or braking system are well know responsible to cause overheating, where extreme attrition of wheel spin are concentrated in a point of the rail (slippage in acceleration) or wheel locked sliding over rail with concentrated attrition in a point of the wheel (slippage in braking), or contact wheel-brake as well. As the heated wheel moves away it is quickly cooled. Another source of overheat are frictions caused deformations know as wheel flat [12]. These sudden thermal oscillations may lead to alter some metallurgical properties of the wheel, where it is observed to incite in cracks and locked in stress of the material [11]. Bearing overheating commonly occurs by gross sliding, where the main causes can be related to lubrication (quality and quantity) and inadequate piece assembly. This overheating leads to decomposition and deterioration of lubricate, reducing ability to lubricate [13]. Inadequate lubrication allows a strong increase of friction that accelerate the degradation of the material.

Overheating events can be classified as faults, since it doesn't directly affect the service during the incident [7] in terms of performance or availability, but accelerates degradation of the material that leads to catastrophic failures. Possibly, there are other hidden causes that this research is seeking and will be better discussed in future papers.

IV. Wayside and Track Sensors Data

Through the use of sensors, condition-based maintenance processes becomes viable by preventing critical failures or degradation in advance [4]. The integration of different data sources in real time can be used to predict (prognosis) and discover latent cause-effect relationships between components (diagnosis). Modern railways are equipped with groups of sensors that generates different measurements about trains and tracks, such as wayside wireless sensors, capable to capture data from cars in movement and track profile measurements captured by instrumented cars with specialized sensors.

For the case study, the following equipment are considered: Hot box and Wheel (HBW) captures thermal emission from wheels and axle boxes (bearings) through infrared sensors; Wheel Impact and Load Detector (WILD) check the force between the rail and moving wheels through the analysis of vertical load in the line. Wheel set Profile (WSP) measure segments of the wheel in order to track abnormal deformations and wear rate. Rail BAM Acoustic Bearing detector (ABD) is an enhanced type of sensor capable to capture acoustic emissions from wheels and bearings and classify possible faults in real time. RB has been strongly used by used by the maintenance team to identity other recurrent faults. Track geometry profile (TGP) measures aspects of the line with focus on detection of deformations and cracks in rails, sleepers and fasteners.

The information comprehend a period of 3 days of simulation measurements. Since the data are spread out in different dataset files and some information are not standardized, some efforts were spent in data handling to generate an appropriate unified dataset for exploration and modeling. It is noticed that HBW are deployed in many points in the line while there is just one appliance of WSP (that also contains WILD data) and ABD located in the same point, since for each record of WSP or ABD, there many records of HBW records for the same wheel/bearing. Another challenge is related to ABD records: For each fault found in the axle it generates a new record. Therefore, for an axle in poor state with x faults, x lines will recorded. Accordingly, a new dataset was generated to merge records from the same axle measurement to able integration with other sensors. The data were integrated in one unified dataset car identification (TAG) and axle number intersection between the sources considering the nearest measurement of WSP/ABD in relation to HBW. Till this date, the authors have no access to TGP data.

V. Partial Results

Based on the unified dataset, an exploratory data analysis are being performed in order to understand the data and identify relationships between the variables. Traditional statistical methods such normality tests (Anderson-Darling, Smirnoff-Kolmogorov, QQ plot), high level descriptions (mean, median and quantiles), linear (Pearson) and non linear (Spearman) correlations, Chi Squared tests, and data

visualization analysis were done. No significant relationship were found. Numerical variables such heating measurements from wheels and bearings are not gaussians with high dispersion and skewness, ranging from 0 to 281 °C and 0 to 50°C, respectively.

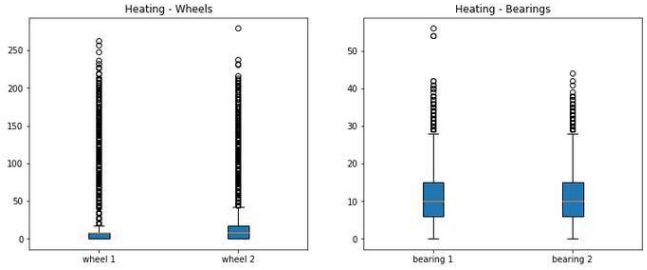


Fig. 1. Wheels and bearings thermal measurements

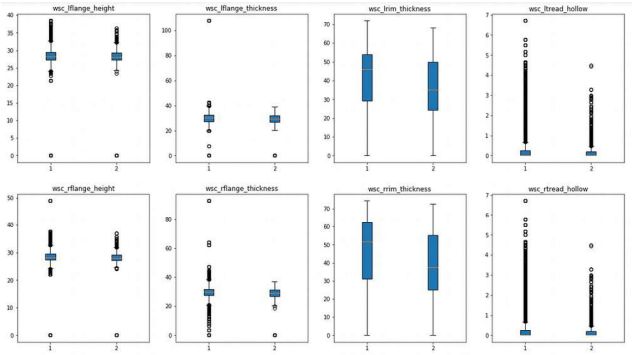


Fig. 2. Wheels profile measurements comparing

Unsupervised methods such K-means, Principal Component Analysis (PCA) and Self Organizing Maps (SOM) were tested in differences ways with objective to create pattern clusters and check the feasibility to map thermal state based on on wheel profile measurements. PCA was tested in two ways: Force dimension reduction in 2 principal components and reduction ensuring 95% of the information. A hand made categorical variable based on hypothetical thermal ranges were create to check the quality in the segregation of overheated records, considering 0 to 18 (normal), 18 to 110 (heating-1), 110 (heating-2) to 180 (heating-3) and greater than 180 °C (heating-4). As shown in figure 2, with limit of 500 plots by cluster some slightly groupings are formed. Due the majority data belongs to normal state and high dispersion of the values, Figure 3 are fully covered. Therefore, no useful information was captured. K-means where tested forcing the creation of 4 clusters using inputs from PCA experiments and raw scaled values, where no results were found in both approaches. Figure 4 shows that centroids are close, showing weak segregation quality. SOM was tested by generating 50×50 and 20×20 nets. Same as PCA and K-means, nothing significant were identified.

Despite the high dispersion of the data, such unclear results might be worsen due some possible reasons. The approach adopted to integrate the data for this unbalanced silos might not be adequate since WSP and ABD datasets are quite infrequent comparing to HBW. Additionally, even applying other interpolation methods, 3 days of measurements might be not enough to understand wear evolution.

Further data considering months or years of measurements over the same axles and cars could facilitate the analysis regarding wear evolution and how it could behaves in overheating problems. However, for the current dataset better data wrangling and integration approaches must be checked. There are many other techniques and details to be explored such, analysis per location, inclusion of external data such as meteorological, track measurements, inspection annotations from maintenance teams.

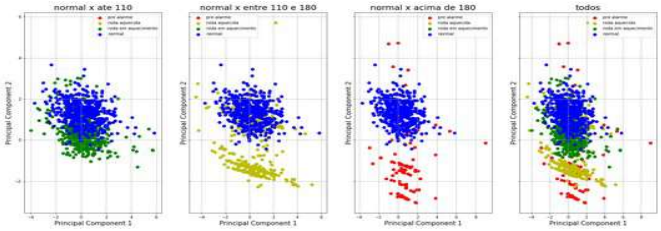


Fig. 3. PCA—500 random points per cluster

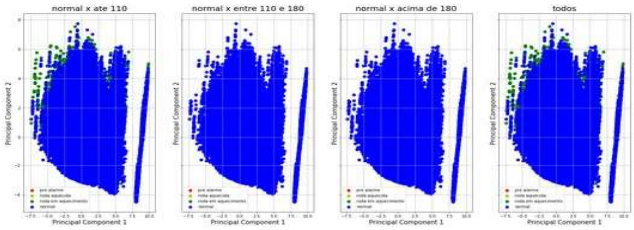


Fig. 4. PCA—All points covered by dispersed ‘normal’ data

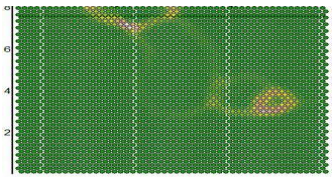


Fig. 4. SOM 50×50

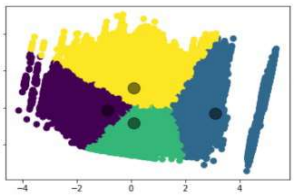


Fig. 5. K-means with 4 clusters

VI. Outlook and Future Steps

Major applications found in the literature leverage combinations of techniques, benefiting from the best of each part. Domain knowledge still important in the analysis, since patterns, deviations or any other interesting detail found in the data could be checked and judged as useful or not by field experts (“correlation does not imply causation”).

The source data considered in the case study are composed by time series measurements from different sensors. Besides the thousands of records from different wheels and bearings, there are few sequential occurrences of the same piece. Moreover, frequency times and records are not standardized between the data sets, since many wayside thermal sensors (known as Hot Box and Wheels—HBW) are spread out in the line while there are few unities from the others. Therefore,

signal-based techniques are not considered in this initial phase till the adequate preparation and integration of the data in a single source.

Deep learning techniques have been seen as state-of-the-art for many complex domains. Latest literature are exploiting interesting approaches in order to capture knowledge from the model representation and bypass the "black box" aspect from neural networks which is fundamental point to be considered for fault diagnosis. Unsupervised learning and dimensionality reduction are robust in order identify partial state faults. PGM techniques are powerful way to structure a stochastic fault chain network, enabling a wider vision about cause-effects relationship. These techniques will be further analyzed and ensemble experiments should be performed. Nevertheless, the research about state of the art applied to fault diagnosis and also applied to overheating in rolling stock must continue and go deeper.

ACKNOWLEDGMENT

The authors would like to thank Vale for the support for this research and for its institutional support to the Safety Analysis Group (GAS), School of Engineering, University of Sao Paulo (Poli-USP).

REFERENCES

[1] MOBLEY, R. K. An introduction to predictive maintenance. Elsevier Science, 2002.

[2] JONGE, B.; TEUNTER R.; TINGA, T. The influence of practical factors on the benefits of condition-based maintenance over time-based maintenance. In Reliability Engineering & System Safety. Special Sections: Reliability and Safety Certification of Software-Intensive Systems, 2017

[3] JUN, H.B.; KIM, D.; A Bayesian network-based approach for fault analysis. Expert Systems with Applications, v. 81, 2017.

[4] LAMPIS, M. and ANDREWS, J. Bayesian belief networks for system fault diagnostics. Quality and Reliability Engineering International, 25, 409–426, 2009

[5] JARDINE, A. K. S.; LIN, D.; BANJEVIC. D. A review on machinery diagnostics and prognostics implementing condition-based maintenance. In: Mechanical Systems and Signal Processing, v. 20, 1483-1510 ,2006.

[6] DE AZEVEDO, H. D. M.; ARAUJO, A. M.; BOUCHONNEAU, N . A review of wind turbine bearing condition monitoring: State of the art and challenges. RENEWABLE & SUSTAINABLE ENERGY REVIEWS v. 56, 368 - 379, March, 2016.

[7] AVIZIENIS, A.; LAPRIE, J.; RANDELL, B.; LANDWEHR C., "Basic concepts and taxonomy of dependable and secure computing," in *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11-33, Jan.-March 2004.

[8] H. REZA, M. PIMPLE, V. KRISHNA and J. HIDLE, "A Safety Analysis Method Using Fault Tree Analysis and Petri Nets," 2009 Sixth International Conference on Information Technology: New Generations, Las Vegas, NV, 2009, pp. 1089-1094.

[9] SICHANI, M. S.; BEZIN Y.; Differential wear modelling – Effect of weld-induced material inhomogeneity on rail surface quality, Wear, v. 406–407,43-52, 2018.

[10] R. ENBLOM. On Simulation of Uniform Wear and Profile Evolution in the Wheel - Rail Contact, PhD dissertation, KTH, Stockholm, 2006.

[11] FLETCHER, D. I.; SANUSI, S. H. The potential for suppressing rail defect growth through tailoring rail thermo-mechanical properties, Wear, v. 366–367,401-406, 2016.

[12] COLE K.D.; TARAWNEH C.M.; FUENTES A.A.; WILSON B.M.; NAVARRO L. . Thermal models of railroad wheels and bearings, International Journal of Heat and Mass Transfer, v. 53, i. 9–10, 1636-1645, 2010

[13] ERDEMIR, A.;BHUSHAN B. . Modern Tribology Handbook, II, CRC Press, 2001, pp. 787–825

[14] TRAN, V. T.; ALTHOBIANI, F.;BALL A.. An approach to fault diagnosis of reciprocating compressor valves using Teager–Kaiser energy operator and deep belief networks, Expert Systems with Applications, v. 41, i. 9,4113-4122, 2014.

[15] SESHADRINATH J.; Singh B.; PANIGRAHI B. K. . "Vibration Analysis Based Inter turn Fault Diagnosis in Induction Machines," in IEEE Transactions on Industrial Informatics, vol. 10, no. 1, pp. 340-350, Feb. 2014.

[16] AL-SHEIKH, H.; HOBLOS, G.; MOUBAYED, N.; NABIL KARAMI. A Sensor Fault Diagnosis Scheme for a DC/DC Converter used in Hybrid Electric Vehicles, IFAC-PapersOnLine, Volume 48, Issue 21, 713-719, 2015.

[17] WANG, Y.; DENG, C.; WU, J.; WANG, Y.; XIONG Y. . A corrective maintenance scheme for engineering equipment, Engineering Failure Analysis, Volume 36,269-283 2014

[18] FENG, Z.;LIANG, M.;CHU, F. Recent advances in time–frequency analysis methods for machinery fault diagnosis: A review with application examples, Mechanical Systems and Signal Processing, v. 38, i. 1,165-205 , 2013.

[19] SONG, W.; SHI, H.; LI Q. Application of Fault Tree Knowledge in Reasoning of Safety Risk Assessment Expert System in Petrochemical Industry, 2009 Pacific-Asia Conference on Knowledge Engineering and Software Engineering, Shenzhen,167-170, 2009.

[20] JAMIL, F.; ABID, M.; HAQ, I.; KHAN, A. Q.; IQBAL, M. . Fault diagnosis of Pakistan Research Reactor-2 with data-driven techniques, Annals of Nuclear Energy, v. 90, 433-440, 2016.

[21] ISERMANN, R.. Fault-diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance. Springer Science & Business Media, 2006.

[22] YONG-KUO, L.; MIN-JUN, P.; CHUN-LI, X.; YA-XIN, D. , Research and design of distributed fault diagnosis system in nuclear power plant, Progress in Nuclear Energy, Volume 68, 97-110, 2013.

[23] GAO, Z.; CECATI, C.; DING, S. X. . A Survey of Fault Diagnosis and Fault-Tolerant Techniques—Part I: Fault Diagnosis With Model-Based and Signal-Based Approaches, IEEE Transactions on Industrial Electronics, vol. 62, no. 6, pp. 3757-3767, 2015.

[24] CAESARENDRA, W.; KOSASIH, B.; TIEU, A. K.; ZHU, H.; MOODIE, CRAIG A.S.; ZHU, Q. . Acoustic emission-based condition monitoring methods: Review and application for low speed slew bearing, Mechanical Systems and Signal Processing, v. 72–73, 134-159, 2016.

[25] AMRUTHNATH, N.; GUPTA, T. . A research study on unsupervised machine learning algorithms for early fault detection in predictive maintenance, 2018 5th International Conference on Industrial Engineering and Applications (ICIEA), Singapore,pp. 355-361, 2018.

[26] LV, F.; WEN, C.; BAO, Z.; LIU, M. . Fault diagnosis based on deep learning, 2016 American Control Conference (ACC), Boston, MA, p. 6851-6856 ,2016.

[27] JIA, F.; LEI, Y.; GUO, L.; LIN, J.; XING, S. . A neural network constructed by deep learning technique and its application to intelligent fault diagnosis of machines, Neurocomputing, v. 272, p. 619-628, 2018.

[28] VERSTRAETE, D.; FERRADA, D.; DROGUETT, E. L; MERUANE, V.; MODARRES, M. . Deep Learning Enabled Fault Diagnosis Using Time-Frequency Image Analysis of Rolling Element Bearings, Shock and Vibration, vol. 2017, Article ID 5067651, 17 pages, 2017

[29] JING, L.; ZHAO, M.; LI, P.; XU, X. . A convolutional neural network based feature learning and fault diagnosis method for the condition monitoring of gearbox, Measurement, v. 111, p. 1-10, 2017.

[30] LECUN, Y; BENGIO, Y; HINTON, G . Deep learning, Nature, 2015.

Interpretability of Knowledge Graph Embedding Models

RUSCHEL, A.*; GUSMÃO, A. C.*; COZMAN, F. G.*
*Escola Politecnica da Universidade de Sao Paulo
E-mail: {andrey.ruschel, arthurcgusmao, fgcozman}@usp.br

***Abstract*—While many chatbot systems rely on templates and shallow semantic analysis, advanced question answering resources are typically produced with the help of large-scale knowledge bases such as DBPedia or Freebase. The state-of-art in information extraction from large knowledge bases turns entities and relations into numeric vectors using low-dimensional mappings called *embeddings*; such embeddings are computationally effective but very difficult to interpret by human users. In this paper we enhance some techniques that aim at turning the outputs delivered by such embeddings into more interpretable answers, thus helping humans to understand and grasp the reasons (or facts) that led to those decisions.**

***Keywords*— Interpretability, embeddings, relational machine learning, knowledge base completio.**

***Classification*— Master's Degree.**

***Category*— Beginner.**

I. Introduction

Embedding techniques are now state-of-the-art in predicting relationships between entities in knowledge bases (KB's) [1]. Such techniques are important in query answering systems needed in advanced chatbots. For instance, suppose that a chatbot must answer the question "Is Company X a subsidiary of Company Y?". The chatbot may turn to a knowledge base containing companies and relationships between them. The state-of-the-art in information extraction from knowledge bases operates using *embeddings*: an embedding is a mapping that transforms entities and relations in the KB into numeric vectors, and represents the existence of relationships as the result of some operation among these vectors. While embeddings usually lead to high accuracy in determining relationships between entities, they are very difficult to interpret. Hence, answers produced through embeddings are hard to justify to a human user. The goal here is to provide tools to improve the interpretability of such answers in chatbot systems and other applications.

The literature has so far failed to consider the interpretability of embeddings of knowledge bases; existing algorithms interpret "complex" classifiers, but embeddings are fairly different from those. In this paper, we will extend the work of Gusmão et. al. [2], and our goal is to evaluate the approach on different knowledge bases and different embedding models. The remainder of this paper is structured as follows: in the section II we provide the required knowledge about *Knowledge Bases*, the most common tasks for *Knowledge Completion*, as well as touching some concepts of *Statistical Relational Learning*. Also, in this section, we provide a review of the main techniques for Knowledge Base Completion subdivided in two major groups, *graph feature* models and *latent feature* models, as well as a description of the approach used to explain embedding models (XKE). Section III provides details of the experiments we have conducted followed by results in section IV and conclusions in section V.

II. Background

In this section we make a very short review of the main concepts related to interpretability, knowledge bases and knowledge graphs.

A. Interpretability

The interest in explainable and interpretable machine learning techniques has exploded in recent years. A turning point was the DARPA program on "Explainable AI", launched in 2016 [3]; since then, several publications and workshops have looked at explainable machine learning. Even though the research on how to explain decisions has a long tradition in artificial intelligence, the sudden recent interest in the topic is due to the fact that extraordinary success has been attained by non-interpretable techniques such as neural networks and embeddings. Users of the latter techniques must be better informed about the reasons behind decisions and recommendations. There has been significant effort to produce explanations out of complex classifiers, often by resorting to global or local approximations by simpler classifiers. The idea there is that the complex classifier is actually used to obtain decisions, but the simpler classifier is learned to produce explanations. For instance, while a deep neural network may be used to classify clients into various categories, the explanation for such classifications is provided by a logistic regression that, in some well-defined sense, approximates the deep neural network [4].

B. Knowledge Bases

Several large-scale knowledge bases (KBs) have been created during the last decade: examples of KBs are NELL [5], YAGO [6], DBpedia [7], WordNet [8] and Freebase [9]. In most of them, information is stored in the form of triples <entity-relation-entity>. Hence a KB has a graph structure where entities are linked through relations. Usually KBs are divided into some groups [10] according to their design: some KBs adopt the *open world assumption (OWA)* (a non-existing triple means that the information is unknown), whereas others adopt the *closed world assumption (CWA)* (a non-existing

triple indicates a non-existing relationship); alternatively, A KB may be *curated* when triples are constructed manually by a group of domain experts, or it may be *collaborative* when constructed by a group of volunteers, or it may be *automated semi-structured* when triples are extracted from semi-structured text, or *automated unstructured* when they are generated automatically by natural language processing algorithms [10].

Knowledge bases are often represented as multigraphs called Knowledge Graphs, where nodes represent entities and edges represent relationships between them.

C. Knowledge Base Completion

To be used in real applications, KBs must be as accurate and complete as possible. In real world applications though, it is very common that those bases are incomplete and store incorrect information. Hence, to tackle this problem, the *Statistical Relational Learning (SRL)* [11] community has been developing a number of approaches focusing in knowledge base completion. Below we describe the more common tasks involving KBs[1]:

1) Link Prediction: this is the task of finding an entity that is related to a given entity plus a relation. In a broader definition, given two instances, find a third one to form a triple.

2) Triple Classification: this task is concerned with discovering if a certain triple (or fact) is true or false. It can be considered as inferring new facts that are not contained in the KB.

3) Entity Resolution: in some KBs built using semi-structured or unstructured schemas, it is common that there are entities represented by different names. Entity resolution or deduplication is concerned with the task of finding such duplicated entities and unifying them.

In this paper we focus in triple classification, leaving other tasks for future work.

D. Statistical Relational Learning

Before entering in the discussion of the two major types of approaches of *SRL* regarding knowledge base completion, it is important to discuss some formal concepts [10]. Let $\varepsilon = \{e_1, ..., e_{Ne}\}$ represent the set of all possible entities of a KB $\mathcal{G}$, and $\mathcal{R} = \{r_1, ..., r_{Nr}\}$ define the set of all known relations. A possible triple can then be defined as $x_{h,r,t} = \langle e_h, r_r, e_t \rangle$ where *h*, *r* and *t* stand for *head*, *relation* and *tail*, respectively. We can then model each triple as a binary random variable $y_{h,r,t} \in \{0, 1\}$ where:

$$y = \begin{cases} 1, & \text{if the triple exists} \\ 0, & \text{otherwise.} \end{cases}$$

For the scope of this paper, we follow the *open world assumption*, and therefore, if $y_{h,r,t} = 0$ means only that the given triple is missing in $\mathcal{G}$, and does not mean that the corresponding fact is false. We can then define $\mathcal{T} = \mathcal{E} \times \mathcal{R} \times \mathcal{E}$ as the set of all the possible triples in $\mathcal{G}$, and $\mathcal{Y} \in \{0, 1\}^{N_e \times R_r \times N_e}$ as the set of all binary random variables. Thus, if we consider $\mathcal{Y}$ a possible world, we can derive the joint distribution $\mathcal{P}(\mathcal{Y})$ from a subset of observed triples $\mathcal{D} \subset \mathcal{T}$.

TABLE I
BENCHMARK DATASETS

Dataset	$\mathcal{E}$	$\mathcal{R}$	$\mathcal{T}$	# Train	# Test	# Valid
FB13	75,043	13	$73 \cdot 10^9$	316,232	5,908	23,733
NELL186	14,463	186	$39 \cdot 10^9$	31,134	5,000	5,000

We can easily see that, for large KBs, $\mathcal{Y}$ can be enormous, even though only a tiny part of it corresponds to true facts. Due to this reason, the best approaches to deal with large KBs are the ones that can better exploit sparcity characteristics.

Below we will discuss the two major classes of approaches to deal with Knowledge Base completion, as stated by Nickel et. al [10]:

1) Graph Feature Models: This approach tries to predict the existence of a triple based only on observable features of the graph, i.e. observed nodes (entities) and edges (relations). Among the variety of algorithms exploiting graph features, in this work we focus in two of them:

- Path Ranking Algorithm:

The Path Ranking Algorithm [12] is based in random walks of bounded lengths to predict links in multi-relational knowledge graphs. More formally, let $\pi_L(i, j, k, t)$ define a path of length L within a graph $\mathcal{G}$. Assuming that $t = (r_1, r_2, ..., r_L)$ represents a sequence of edge types within a path $e_i \rightarrow e_2 \rightarrow e_3 \rightarrow ... \rightarrow e_j$, and that there is a relation r_k connecting e_i and e_j. We can then let $\Pi_L(i, j, k)$ represent all possible paths of length L, ranging over path types t. The probability $P(\pi_L(i, j, k))$ of following a given path can be computed recursively by a sampling procedure. The path probabilities are used as features for predicting the probability of missing edges. More formally, the feature vector can be represented as $\phi_{ijk}^{PRA} = [P(\pi) : \pi \in \Pi_L(i, j, k)]$. Using a logistic regression $f_{ijk}^{PRA} := w_k^T \phi_{ijk}^{PRA}$ it is possible to predict edge probabilities, i.e., new facts on the knowledge base.

- Subgraph Feature Extraction:

Subgraph Feature Extraction [13] is an improvement of *PRA* with better performance, also exploiting graph features. Let π denote a path type formed by some random sequence of edges $r_1 \rightarrow r_2 \rightarrow ... \rightarrow r_i$ within a knowledge graph $\mathcal{G}$. SFE builds a subgraph $\mathcal{G}_n$ centered around each entity $e_n \in \mathcal{G}$ using k random walks.Each random walk leaving e_n forms a path $\pi_{n,i}$ reaching an intermediate node e_i. Then, similarly to PRA, a feature vector is built for each source target pair (e_n, e_m) by merging the subgraphs $\mathcal{G}_n$ and $\mathcal{G}_m$ at the intermediate nodes e_i. All combinations of path types $\pi_{n,i}$ and $\pi_{m,i}$ for each e_i are stored as binary feature vectors that are later combined into a feature matrix that can be used as input for any supervised classifier.

2) Latent Feature Models: The models that use latent features, also called *embeddings* are models that convert entities and relations into low-dimensional vectors within a continuous space. The key here is that they allow simplifications in the calculations while preserving the inherent characteristics of the

TABLE II
RESULTS (MICRO-AVERAGE) FOR BOTH XKE VARIANTS / EMBEDDING MODELS.

Dataset	**FB13**				**NELL186**			
Embedding Model	**TransE**		**Analogy**		**TransE**		**Analogy**	
XKE variant	**TRUE**	**PRED$_5$**	**TRUE**	**PRED$_5$**	**TRUE**	**PRED$_5$**	**TRUE**	**PRED$_5$**
Embedding Accuracy	82.55		73.83		86.40		92.78	
# Positive triples in $\mathcal{G}$ (XKE-TRUE) or $\hat{\mathcal{G}}$ (XKE-PRED)	322k	1,668k	322k	2,438k	36k	524k	36k	665k
$\hat{\mathcal{G}}$ positive over predicted ratio	-	0.168	-	0.303	-	0.581	-	0.736
# Features per example	2.91	1.34	2.91	2,62	70.66	249.86	70,36	227,66
% Examples with # features > 0	54.73	37.88	54,73	47,75	50.01	45.57	50,12	56,36
Explanation Mean # Rules (for explanations with size > 0)	2.29	2.70	3.94	3.64	51.33	159.02	59.45	77.38
Explanation Mean Rule Length	3.09	2.87	3.16	3.02	3.86	3.89	3.81	3.83
Fidelity	73.26	74.36	78.67	77.30	86.55	74.94	91.01	86.58
Fidelity (filtered for examples with # features > 0)	80.52	85.74	76.97	80.20	87.02	83.07	92.62	91.59
Fidelity (weighted by the # features)	75.21	84.58	79.93	79.74	85.66	86.24	97.59	94.38
Accuracy	73.43	71.78	72.41	68.29	89.10	76.18	90.57	85.46
Accuracy (filtered for examples with # features > 0)	80.78	82.02	80.54	81.41	91.19	84.30	94.51	90.92
Accuracy (weighted by the # features)	71.68	81.28	83.09	83.06	82.12	89.11	97.90	94.96
F1 (Fidelity)	76.66	71.14	80.65	75.31	83.19	68.07	88.68	80.51
F1 (Accuracy)	77.35	69.16	76.66	68.71	86.89	71.14	89.07	80.22

knowledge graphs[1]. Several models have been developed in the recent years, but in this work we focus on two of them, namely *TransE* [14] and *Analogy* [15].

- TransE:

Inspired by models such as Word2Vec [16], this is a very simple and yet effective model. Entities and relations are represented within the same low-dimension vector space, and relations are translations within that space. More formally[14], let two entities e_h and e_t be represented by two low-dimentional vector $\mathbf{h}$ and $\mathbf{t}$ in $\mathbb{R}^N$, and let a relation r be represented by a vector $\mathbf{r}$ in the same space. We can say that the triple (h, r, t) holds when $h + r \approx t$ with low error.

- Analogy: Analogy [15] is another *latent feature* model that is capable of building latent representations that are able to capture the *analogical* properties of the embedded entities and relations. Following the notation above, let $\mathcal{E}$ and $\mathcal{R}$ represent the space of entities and relations of a knowledge base $\mathcal{G}$, where $h \in \mathcal{E}$, $t \in \mathcal{E}$, $r \in \mathcal{R}$ are *head*, *tail* and *relation*, respectively. Also, let $v \in \mathbb{R}^{|R| \times m}$ define a look-up table where $v_e \in \mathbb{R}^m$ represents the vector embedding for entity e. Analogically, $W \in \mathbb{R}^{m \times m \times m}$ is a tensor where $W_r \in \mathbb{R}^{m \times m}$ is the embedding matrix for relation r. The goal is to learn v and W from $\mathcal{G}$ in a way that for any valid triple $\langle h, r, t \rangle$ the equation $v_h^\intercal W_r \approx v_t^\intercal$ is satisfied. The score function $\phi(h, r, t) = \langle v_h^\intercal W_r, v_t \rangle = v_h^\intercal W_r v_t$ must yield higher scores for valid triples and lower scores to invalid ones.

E. Explaining Knowledge Embedding Models

We now review the approach proposed by Gusmão et. al [2], applying SFE to build a more interpretable model that explains embedding models. The techniques proposed are inspired in pedagogical approaches developed isince the 1990s [17], combining a very complex and good classifier (that is poorly interpretable) with a simpler classifier to explain the decisions.

- XKE-PRED (Explaining Knowledge Embedding Models with Predicted Features): This is the more direct application of a pedagogical approach. Here the embedding model is considered a black-box, meaning that for the explainable classifier we assume no other source of information. Running the *SFE* algorithm in the data from the embedding model, the features generated can be combined with the labels predicted by the embedding model to create a matrix of features that can be used as input to a logistic regression classifier. This logistic regression will be the source of the explanation in the form of weighted Horn clauses. Defining the model formally, let $\mathcal{T} = \mathcal{E} \times \mathcal{R} \times \mathcal{E}$ denote, following notation adopted above, the set of all possible triples in a knowledge graph $\mathcal{G}$. $\Pi_\mathcal{G}$ is the set of all possible paths between two entities, and $P(\Pi_\mathcal{G})$ its power set. The original black-box classifier is denoted by $g : \mathcal{T} \to \{0, 1\}$, and the feature extraction function generated by SFE is denoted by $F : \mathcal{T} \to P(\Pi_\mathcal{G})$, for a triple $x_{h,r,t} \in \mathcal{T}$. The model is generated by constructing a set of n examples $\mathbb{D}' = \{F(x_{h,r,t} \mid \hat{\mathcal{G}}), g(x_{h,r,t}))\}^n$ that will be used to train the interpretable classifier $g' : P(\Pi_{\hat{\mathcal{G}}}) \to \{0, 1\}$, where $\hat{\mathcal{G}} = \{g(x_{h,r,t} \mid x_{h,r,t} \in \mathcal{T})\}$ is the graph containing all the triples predicted as true facts by $g(\cdot)$. Explanations are drawn from $g'(\cdot)$ as a function of $P(\Pi_{\hat{\mathcal{G}}})$.

- XKE-TRUE (Explaining Knowledge Embedding Models with Observed Features): It is a variation of the previous approach, with the difference that it assumes an external source of information besides the embedding model. In this method, explanations of the black-box's predictions are based on features observed from the original graph, not from the embedding model itself. More formally, a set of n examples $\mathbb{D} = \{F(x_{h,r,t} \mid \mathcal{G}), g(x_{h,r,t}))\}^n$ is constructed and it is used as input to an interpretable classifier $g'' : P(\Pi_\mathcal{G}) \to \{0, 1\}$, from which explanations are drawn as a function of $P(\Pi_\mathcal{G})$.

We can see from TABLE I that the number of possible triples is huge, so the model resorts to applying k-nearest neighbors to find existing triples by entity similarity. By doing so the search space is reduced and becomes tractable. More formally, let $\mathcal{T}_0$ be a random sample obtained from $\mathcal{T}$. An extension of this subset, $\mathcal{T}_0^k$, is generated by corrupting

both entities (head and tail) for each triple predicted as correct in $\mathcal{T}_0$ with its k nearest neighbors. Then, we obtain $\hat{\mathcal{G}}_0^k = \{g(x_{h',r,t'}) \mid x_{h,r,t} \in \mathcal{T}_0^+ \wedge e_{h'} \in N_k(e_h \mid \Theta_g) \wedge e_{t'} \in N_k(e_t \mid \Theta_g)\}$ that is the set of correct triples inferred by the classifier $g(\cdot)$, where $N_k(e \mid \Theta_g)$ represents the subset constructed by e and its $k-1$ nearest neighbors, and Θ_g is the vector formed by the entities.

III. Experiments

In a previous work [2], Gusmão et. al applied **XKE-PRED** and **XKE-TRUE** over the results of the embedding model **TransE** learned over the datasets **FB13** and **NELL186** (shown Table I). In this paper, we expand their work by applying both XKE variants to **Analogy** models learned over the same datasets, aiming to investigate and compare performances. Both embedding models were trained via grid search, limited to 1.000 epochs, and negative triples were generated using the Bernoulli distribution method in a rate of two negative triples for each positive example. Even tough we tested entity similarity for nearest neighbors using $k = 3$, 5 and 7, due to space constraints we report only results for $k = 5$.

Regarding performance, metrics we consider are:

- fidelity: the ability of the pedagogical method to mimic the behavior of the embedding model. More formally, let us denote $\mathcal{D}_{test}$ a set of test triples. Let $\hat{y}_g$ denote a prediction made by an embedding model for a given input triple $\langle e_h, r_r, e_t \rangle \in \mathcal{D}_{test}$ and $\hat{y}_{XKE}$ the prediction made by XKE for the same triple. Fidelity can be computed as $\mathbb{P}(\hat{y}_{XKE} = \hat{y}_g) = \sum_{x \in \mathcal{D}_{test}} \frac{1-|\hat{y}_{XKE} - \hat{y}_g|}{|\mathcal{D}_{test}|}$.
- accuracy: the ability of the weighted rules to correctly predict real data. More formally, let $\hat{y}$ denote a prediction of a given classifier, y a binary random variable that models the existence of the same instance, and $\mathcal{D}_{test}$ a test set. Accuracy can be computed by $\mathbb{P}(\hat{y} = y) = \sum_{x \in \mathcal{D}_{test}} \frac{1-|\hat{y}-y|}{|\mathcal{D}_{test}|}$.

And for interpretability, two metrics are considered:

- # of rules with weight greater than zero;
- mean rule lenght.

The embedding models' performance is presented in TABLE II. With regards to accuracy, Analogy over FB13 had a much worse performance than TransE, whilst over NELL186, it performed much better. We suspect that the intrinsic topology of each dataset directly influences the embedding model performance, but this analysis is beyond of the scope of this paper. We can see that, for $\hat{\mathcal{G}}$ triple generation, Analogy performed better than TransE for XKE-PRED. This increase in performance was dramatic in FB13 and more subtle in NELL186. Regarding accuracy, we can see that, considering only examples with more than one feature extracted, both methods obtained a similar performance in FB13 and a better performance in NELL, similar behavior found for fidelity. With regard to interpretability, the explanation mean rule is less than four, due to a constraint imposed for performance reasons, and the number of rules extracted remained almost the same for FB13, and decreased for NELL186, turning the interpretation simpler using Analogy in contrast to TransE.

IV. Conclusion

We can see that both XKE-PRED and XKE-TRUE can be applied over datasets FB13 and NELL186 using Analogy embedding model with good results, meaning that XKE can model the new facts inferred by the embedding model with good fidelity. So far we tested only two datasets and two different embedding models, for future work, expanding this analysis would be a good line of research. Another interesting line would be to investigate the intrinsic structure of different benchmark datasets, to understand how its differences influence both the performance of the embedding model itself, as well as the performance of XKE.

Acknowledgement

This work was accomplished with the support from Itaú Unibanco S.A., through the scholarship program *PBI - Programa de Bolsas Itaú* together with the *C2D - Centro de Ciência de Dados* from *EPUSP - Escola Politécnica da Universidade de São Paulo*. Second author is supported by an agreement between IBM and the Sao Paulo Research Foundation (FAPESP) (grant 2017/19007-6). The project received financial support from FAPESP (grant 2016/18841-0). The third author is partially supported by CNPq (grant 308433/2014-9).

References

[1] WANG, Q. et al. Knowledge Graph Embedding : A Survey of Approaches and Applications. *IEEE Transactions on Knowledge and Data Engineering*, v. 29, n. 12, p. 2724–2743, 2017.

[2] GUSMÃO, A. C. et al. Interpreting Embedding Models of Knowledge Bases : A Pedagogical Approach. n. Whi, 2018.

[3] GUNNING, D. *Broad Agency Announcement Explainable Artificial Intelligence (XAI)*. [S.l.], 2016. DARPA–BAA–16–53 p.

[4] RIBEIRO, M. T.; SINGH, S.; GUESTRIN, C. "Why Should I Trust You?": Explaining the Predictions of Any Classifier. 2016. ISSN 9781450321389.

[5] MITCHELL, T. et al. Never-Ending Learning. *Communications of the Acm*, v. 61, n. 1, p. 2302–2310, 2015.

[6] SUCHANEK, F. M.; KASNECI, G.; WEIKUM, G. YAGO: A Core of Semantic Knowledge Unifying WordNet and Wikipedia. *WWW 2007*, 2007.

[7] LEHMANN, J. et al. *DBpedia - A Large-scale, Multilingual Knowledge Base Extracted from Wikipedia*. [S.l.], 2012. v. 1, 1–5 p.

[8] MILLER, G. A. *WordNet: A Lexical Database for English George A. Miller*. 1995. 39–41 p.

[9] BOLLACKER, K. et al. *Freebase: A Collaboratively Created Graph Database For Structuring Human Knowledge*. [S.l.], 2008. 1247–1249 p.

[10] NICKEL, M. et al. *A Review of Relational Machine Learning for Knowledge Graphs*. [S.l.], 2015.

[11] GETOOR, L.; TASKAR, B. *Introduction to Statistical Relational Learning (Adaptive Computation and Machine Learning)*. [S.l.]: The MIT Press, 2007. ISBN 0262072882.

[12] LAO, N.; COHEN, W. W. Relational Retrieval Using a Combination of Path-Constrained Random Walks. *Machine Learning*, v. 81, n. n.1, p. 53–67, 2010.

[13] GARDNER, M.; MITCHELL, T. Efficient and Expressive Knowledge Base Completion Using Subgraph Feature Extraction. p. 1488–1498, 2015.

[14] BORDES, A. et al. Translating Embeddings for Modeling Multi-Relational Data. *Advances in NIPS*, 2013. ISSN 10495258.

[15] LIU, H.; WU, Y.; YANG, Y. Analogical Inference for Multi-relational Embeddings. 2017.

[16] MIKOLOV, T. et al. Efficient Estimation of Word Representations in Vector Space. 2013.

[17] ANDREWS, R.; DIEDERICH, J.; TICKLE, A. B. *Survey and critique of techniques for extracting rules from trained artificial neural networks*. [S.l.], 1995. 373–389 p.

CBLP: a case-based approach to predict human mobility

Silva, C. I. L. C. ; Brandão, A. A. F. Siqueira, F. L. †;
Laboratório de Técnicas Inteligentes - Escola Politécnica - USP
†Laboratório de Tecnologia de Software - Escola Politécnica - USP
E-mail: igortkd2006@gmail.com {anarosa.brandao, levy.siqueira}@usp.br

Abstract—Nowadays, there are several devices that can provide GPS information continuously. The availability of all this information combined with the improvement of techniques to analyze massive amount of geolocation data opens up new possibilities of services related to human mobility. Smart traffic control, safety planning routes, and smart and safe driving are among the domains that can benefit from models to predict human mobility. In this paper we present a new approach to predict human mobility based on Case Based Reasoning (CBR). Using the Geolife GPS dataset to apply and analyze our proposal, we obtained as result 72% of accuracy, a value similar to the obtained by other studies. Our conclusion is that CBR can be successfully applied to geolocation prediction. Moreover, there are still many improvements that can greatly improve its accuracy.

Keywords— geolocation prediction, case based reasoning, data mining, mobility big data.

Classification — Master's degree.

Category— Beginner

I. Introduction

The massive amount of geolocation personal data can provide useful information about user's mobility. Nowadays the user's historical location can be provided by devices with embedded geolocation position systems (GPS) such as smart phones, navigators, trackers, notebooks, wearables, vehicular navigation systems, and others [1]. The wide variety of devices and their ability to generate records in short intervals, 1 to 5 seconds [2] [3], [4] enables the collection of massive amount of geolocation data and introduces the concept of Mobility Big Data (MBD) [1].

Geolocation data can feed Geolocation Prediction Models (GPM) [1] in order to predict personal information about a next geolocation based on current geolocation. Moreover, the MBD analysis can provide meaningful inputs to the GPM, e.g. information about the region where the user is at the moment may have more value to the model than a GPS point (latitude, longitude and altitude). According to Xu et al [1], this combination of GPM and MBD can provide or improve several location-based services such as smart traffic control, safety planning routes, resources recommendations, smart and safe driving, social interaction, personalized notifications, among others.

In a recent survey, Xu et al. [1] categorize solutions to GPM associated with MBD as: (i) Markov-based methods; (ii) Bayesian network-based methods; (iii)Neural Networks-based methods; and (iv) Regression-based methods. The use of such approaches present an average accuracy that range from 39% to 78% [1]. Nevertheless, Lu et al [5] and Song et al [6] presented that human mobility is 93% and 95% predictable respectively, which means that there is still room to improve the average accuracy of GPM.

In this paper we propose CBLP, an CBR approach to estimate geolocation prediction. The CBLP results in a real life dataset indicates a promising method that should be more explored. This document is organized as follows: section II presents some background for understanding our proposal; section III some existing work on the theme; section IV our proposal and section V the application of our model to a dataset. In section VI we present the evaluation of our model and associated results and, finally, our conclusions and future work in section VII.

II. Background

A. Mobility Big Data Analysis

Mobility Big Data analysis consists of processing and clustering geolocation raw data into popular geolocation regions (PGR), followed by mining personal trajectories (PT) from the PGR's [1]. In order to apply our approach, Geolife [4], a dataset containing mobility raw data, was chosen as the data source, and DBSCAN as the algorithm for clustering such data. Having the clusters, each PGR is represented by the cluster it belongs and PT are mined considering clusters as abstractions to their starting, middle and ending PGR's [1].

1) Mobility Dataset: Geolife is a GPS trajectory Dataset collected by Microsoft Research on Asia. It contains data from 182 users collected from 2007 to 2012 and describes more than 17 thousands trajectories. The Geolife database is composed of several files each one representing one or more trajectories on a specific day for a specific user. By trajectory we mean a sequence of records where the difference between two subsequent records is at most 300 meters or 30 minutes. Its files contain logs of location and time records. Each record is represented in a row and composed by seven fields: latitude, longitude, 0, altitude, #days from 12/30/1899, date, time. The number of records in Geolife dataset is $23.42 \quad 10^6$.

2) Clustering Algorithm: The density-based spatial clustering of applications with noise (DBSCAN) algorithm [7] is a clustering algorithm that groups points that are closely packed with a minimum near points and mark as noise points alone in a region with few near points. DBSCAN require two

parameters to be executed: EPS and MinPoints. EPS defines that a point *P* is part of a cluster *C*, whenever the distance from *P* to any existing point of *C* is equal or less than EPS. The MinPoints defines the density of the clusters and determine the minimum density of points necessary to form a cluster.

3) Mining Trajectories from Clusters: Mining a trajectory from clusters consists of reducing dimensionality by obtaining a personal trajectory (PT) based on popular geolocation region (PGR).Therefore, having a GPS dataset such as Geolife, mining a representation of a GPS trajectory to a PT basically consists of mapping the dataset geolocation records to a sequence of PGR where each geolocation record belongs. An example of a trajectory dimensionally reduced is: PT = $< ClusterA, ClusterB, ClusterA >$.

B. CBR: Case Based Reasoning

CBR is Artificial Intelligence approach to solve problems based on similar past cases [8]. A CBR system solves new problems (target problems) by adjusting or using solutions from old problems (analogue problems) [9].The CBR methodology have four main steps: (i) retrieve similar analogue cases to the target problem; (ii) reuse analogue solutions to propose a new solution to the target problem; (iii) revise if necessary to improve the solution of target problem; and (iv) retain the new solution to improve knowledge.

Some advantages of using CBR are: (i) only deal with real problems avoiding to worry about all possible problems; (ii) handle risk cases by identifying scenarios with high error degree; (iii) there is no need of having a good understanding about scenario domain because solutions are based on past cases data collected; (iii) large number of solution applied to different domain including recommendation systems.

III. Related Work

Ashbrook [10] used Markov models to calculate a matrix of probabilities of movements between locations. They collected the data used in experiments and they did not exposed average accuracy for all users.

Herder et al [11] implemented a method that use probabilistic functions, Markov methods and closest locations to the user current location to predict the next location. Their work applied techniques used to predict revisitations in websites to geolocation prediction. They state the existence of a strong dependence between destinations and period of the day and use it as an additional input to their method. Moreover, they adopted Geolife as the dataset and considered that each dataset file contains only one user trajectory. Such choice can hide important information, where an interval of more than 60 minutes may indicates the end and the beginning of two subsequent trajectories.

Khoroshevsky and Lerner [12] proposed a method based on probabilistic functions to compute the location prediction. Geolife was chosen as the dataset. Diversely from [11], they pre-processed the dataset to shrink it while maintaining the utility of information collected in its files. Therefore, they established a limit of 20 minutes and 50 meters between subsequent records in a file as a way to discard trajectory middle points. We advocate that by using such limits they may have discarded starting and ending points of trajectories, since a Geolife file may contain more than one trajectory in a file.

Gambs et al [13] used Markov method to predict if a user is at home, at work, or at other place. They use a probabilistic method based on user's last visitations to predict the next locations. Their approach is limited in respect to the possibilities of different destinations.

Different from methodologies cited above our approach strongly depends on finding similar cases to the target trajectory. Naturally, more data should result in more assertive choices for similar cases, but our model does not need to limit the amount of data necessary to execute the prediction. In other words our approach accuracy is not restricted by a big amount of data, but by the similarity of data.

IV. The Case-Based Location Prediction Model (CBLP)

The CBLP is based on CBR and it is composed of two steps extracted from CBR: (i) retrieve most similar analogue trajectories to a target trajectory; (ii) reuse analogue data to predict the target trajectory. Our model assumes that the most similar the trajectories are, the greater the likelihood of their destination be the same. These assumptions considers that human mobility is strongly influenced by past behavior [5]. An overview of our model is presented in figure 1.

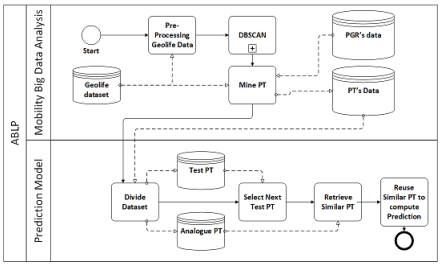


Fig. 1: Case Based Location Prediction (CBLP) Model.

A. Retrieve Similar Trajectories

In order to retrieve similar analogue trajectories it is necessary to define some distance to compare trajectories. Similarity is evaluated by calculating the distance between each analogue trajectory and the target one. The closest ones are considered similar to the target. We used the ED to measure the similarity. To properly use ED it is necessary to convert a trajectory into an n-dimensional array containing features with high relevance to the trajectory destination. According to [6], [14] in most cases human mobility are re-visitations with high temporal and spatial regularity, because Geolife is composed exactly with spatial and temporal data this understanding justifies the use Geolife of predict mobility. Focusing on comparing and retrieving similar trajectories is possible to infer several inputs from Geolife data such as the nearest buildings or places for spatial attributes and the day of week or period of the

TABLE I: Time features to numbers

Time feature	Symbol	Number
Period of the day	AM/PM	0/1
Day type	Week/Weekend Day	0/1
Day of the week	Mon/Tue/Wed/Thu/Fri/Sat/Sun	0/1/2/3/4/5/6

Source: Adapted

day for temporal attributes. All these features can be used to characterize a trajectory focusing on space and time.

We use latitude and longitude because the ED of geolocation attributes are proportional to the geographic distance, this means the closer to 0 is the ED between two trajectories' spatial attributes, the more geographic closer are the trajectories' points.

According to Herder, Siehndel and Kawase [11], trajectory destination (end point) is dependent on the time of day which the trajectory begins (start point) and it is also dependent on the type of day it occurs (week or weekend). Based on this understanding, we also defined the features (i) period of the day (AM or PM), (ii) day type (weekday or weekend day), and (iii) day of the week (Monday, Tuesday, ..., Sunday) for representing the time attributes which represent a trajectory. Both attributes (time and geolocation) refer to the starting point of a trajectory and were obtained at the moment of mining PT's. Then, we assign numerical values to each time feature, as indicates table I. Since time features and geolocation attributes are represented using different units, a normalization is necessary to ensure that each attribute has the same impact on the result.

An example of the normalized array is given by

$$< 0, 0.00854, 0.03342, 0.45609, 0.97231 >,$$

where the array entries represents, respectively, the period of the day; the day type; the day of the week; the latitude of the starting point; the longitude of the starting point. Having calculated the distance between each analogue trajectory to the target one, we consider the closest three as the similar analogue trajectories.

B. Reuse Similar Trajectories

The reuse of similar trajectories to derive the next destination considers the fact that they have similar features of time and space of the target trajectory by construction. Therefore, the algorithm has to choose, among the similar analogue trajectories, a single one to serve as the derived solution. Whenever possible, our algorithm chooses the most frequent (the mode) among the most similar analogues to the target trajectory, otherwise, it chooses the one most similar analogue.

V. Applying CBLP to Geolife

A. Geolife Data Analysis

In order to apply our approach to Geolife, we first need to conduct the MBD analysis to it and extract the PGR's and PT's for each user. These steps are applied to all dataset with no restrictions. We already defined on section II our understanding of what is a trajectory as well as the algorithm used to cluster points into PGR, the DBSCAN. To implement DBSCAN we use the Apache Machine Learn Library [15]. In addition, for the purpose of avoiding DBSCAN performance issues while running with large datasets, we decided to discard middle points of all trajectories, following the approach already adopted by [12]. By doing this, the number of records to be clustered by DBSCAN decrease from $23.42 * 10^6$ to $1.09 * 10^5$.

As aforementioned, the algorithm requires EPS and MinPoints as input parameters. Nevertheless, such values impacts the result of the DBSCAN execution depending on the number of records for a user. In order to mitigate the impact of the choice for EPS and MinPoints values in the algorithm accuracy, we ran DBSCAN for EPS ranging from 5 to 30, with a step of 5 units, for each user. Also, MinPoints are set to range from 1 to 4, because we do not want to restrict the creation of a new cluster. Since all points are departures or destinations, larger values of MinPoints may exclude locations that were visited just a few times.Therefore, all combinations for (Users, EPS, MinPoints) were considered to generate the dataset that serves as input for CBLP resulting in 24 (6 EPS * 4 MinPoints) experiments executed for each user.

Mining PT follows the approach described on section II-A3 and the resulting data serve as input for the Prediction Model of CBLP. A total of 62544 PT populate the PT dataset.Having the personal trajectories (PT) yielded by the Geolife data analysis, the next step is applying the Prediction Model to them. Therefore, retrieving and reusing similar trajectories are the steps to be conducted using the PT dataset.

B. Retrieving similar trajectories

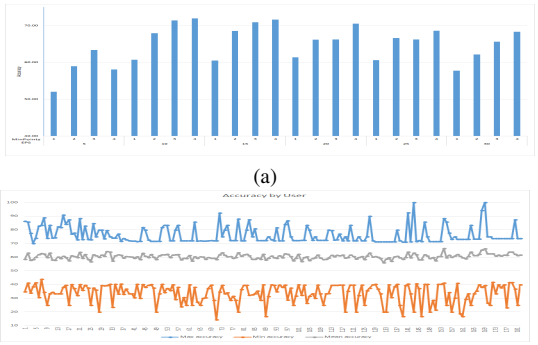
In order to prepare PT data to apply the prediction model, we split the resulting data from each user into two parts chronologically ordered: the first $\frac{2}{3}$ of PT were considered as analogue cases and the last $\frac{1}{3}$ of PT were considered as targets to be predicted. The retrieving process consists of, for each target PT, evaluating similarity between the target PT and all analogue PT and selecting the three most similar PT.

C. Reusing similar trajectories and deriving destination

For each target, from the three most similar trajectories, we verify if there is overlap of destinations. If so, we chose as the target destination the most frequent one, otherwise we choose the target destination as the one from the most similar trajectory.

VI. Evaluation and Results

In order to evaluate our model we perform the steps described in section V for each of the 4368 (=182*6*4) combinations of users, EPS and MinPoints, performed in the time of 3 days. Therefore, executions with less than 10 personal trajectories (at least 7 considered as analogues and 3 as targets) were ignored to avoid trending data. Each one execution has a set of destinations to be predicted and the success of prediction will be given by the comparison of the predicted destination with the ones of the target PT dataset. Accuracy was calculated considering the ratio between the



(a)

(b)

Fig. 2: A - Accuracy due to EPS and MinPoints. B - Accuracy results performed by each user.

TABLE II: Prediction Accuracy Models

Author	Dataset	Locations per user	Accuracy
CBLP	Geolife (182 users)	12	0.72
Gambs et al., 2012	Geolife (175 users)	8	0.7 - 0.95
Khoroshevsky and Lerner[1]	Geolife (168 users)	4	0.82
Khoroshevsky and Lerner[2]	Geolife (168 users)	19	0.75

Source: Adapted from Khoroshevsky and Lerner.

number of successful prediction ($Succ$) and the total number of target trajectories ($Total$).

Figure 2 presents a plot with the results of all experiments performed. Each column represents the results of the average accuracy for all users, considering an specific value for EPS and MinPoints. By analyzing the plot, we may infer that the best values of (EPS, MinPoints) DBSCAN parameters, considering the accuracy ($> 70\%$), were (10,4), (15,4), (10,3) and (15,3). If we consider the our best combination for EPS and MinPoints, our accuracy is 72%. Nevertheless, since we execute all the possible combinations of (EPS,MinPoints) for each user, we also calculate the mean average accuracy for all of them, which results in 60.51%.Figure 2B presents the Max, the Average, and the Min results of accuracy for all DBSCAN parameters, with each point representing a user.

A comparison with existing work that used Geolife is presented in table II and as we see, our approach did not overcome [12] or [13], but some considerations are relevant. When comparing to [12], their best results improve ours by 10% and this difference can be justified by the difference in locations discovered by user. If the cluster process generates a few numbers of locations as possible destinations, it is reasonable that your accuracy will be improved because, statistically, there is a greater probability of success. When comparing with [13], it is important to remark that their results are displayed for 3 different datasets, but specifically for Geolife their accuracy ranges around 60% - 70% so CBLP overcome [13] specifically for Geolife.

VII. Conclusion

Accurate prediction of user's mobility can improve services based on geolocation. In this paper we proposed CBLP, an case-based model to predict the human mobility. Although CBLP does not overcome other approaches to the same problem, the accuracy calculated under the same basis is close of existing work that adopts the same dataset. This was our first incursion of using a CBR-based approach in such a domain and our choices were the simple ones, mainly to check if it could be promising or not.

Differently from others our method is not probabilistic avoiding restrictions about amount of data. Probabilistic methods like Markov or Bayesian are the most widely used according to Xu *et al*. To our understanding, encouraging new approaches is crucial to improve the field research. The results encourage us to advocate that CBLP was successfully applied in the human mobility and that there is room to improve it. In fact, Aamodt and Plaza [8] argue that the retrieving step of a CBR cycle could provide better results with the adoption of techniques such as nearest neighbor, induction, statistics, neural networks, fuzzy logic, etc. Improvements may also come from the inclusion of the revise and retain steps of the CBR cycle in the CBLP model.

References

[1] XU, G. et al. A survey for mobility big data analytics for geolocation prediction. *IEEE Wireless Communications*, IEEE, v. 24, n. 1, p. 111–119, 2017.

[2] WU, X. et al. Data mining with big data. *ieee transactions on knowledge and data engineering*, IEEE, v. 26, n. 1, p. 97–107, 2014.

[3] ZHENG, Y. et al. Understanding mobility based on gps data. In: ACM. *Proceedings of the 10th international conference on Ubiquitous computing*. [S.l.], 2008. p. 312–321.

[4] ZHENG, Y.; XIE, X.; MA, W.-Y. Geolife: A collaborative social networking service among user, location and trajectory. *IEEE Data Eng. Bull.*, Citeseer, v. 33, n. 2, p. 32–39, 2010.

[5] LU, X. et al. Approaching the limit of predictability in human mobility. *Scientific reports*, Nature Publishing Group, v. 3, p. srep02923, 2013.

[6] SONG, C. et al. Limits of predictability in human mobility. *Science*, American Association for the Advancement of Science, v. 327, n. 5968, p. 1018–1021, 2010.

[7] ESTER, M. et al. A density-based algorithm for discovering clusters in large spatial databases with noise. In: *Kdd*. [S.l.: s.n.], 1996. v. 96, n. 34, p. 226–231.

[8] AAMODT, A.; PLAZA, E. Case-based reasoning: Foundational issues, methodological variations, and system approaches. *AI communications*, IOS press, v. 7, n. 1, p. 39–59, 1994.

[9] WATSON, I. Case-based reasoning is a methodology not a technology. *Knowledge-based systems*, Elsevier, v. 12, n. 5-6, p. 303–308, 1999.

[10] ASHBROOK, D.; STARNER, T. Using gps to learn significant locations and predict movement across multiple users. *Personal and Ubiquitous computing*, Springer, v. 7, n. 5, p. 275–286, 2003.

[11] HERDER, E.; SIEHNDEL, P.; KAWASE, R. Predicting user locations and trajectories. In: SPRINGER. *International Conference on User Modeling, Adaptation, and Personalization*. [S.l.], 2014. p. 86–97.

[12] KHOROSHEVSKY, F.; LERNER, B. Human mobility-pattern discovery and next-place prediction from gps data. In: SPRINGER. *IAPR Workshop on Multimodal Pattern Recognition of Social Signals in Human-Computer Interaction*. [S.l.], 2016. p. 24–35.

[13] GAMBS, S.; KILLIJIAN, M.-O.; CORTEZ, M. N. del P. Next place prediction using mobility markov chains. In: ACM. *Proceedings of the First Workshop on Measurement, Privacy, and Mobility*. [S.l.], 2012. p. 3.

[14] GONZALEZ, M. C.; HIDALGO, C. A.; BARABASI, A.-L. Understanding individual human mobility patterns. *nature*, Nature Publishing Group, v. 453, n. 7196, p. 779, 2008.

[15] APACHE, S. F. *Math – The Commons Math User Guide - Machine Learning*. Disponível em: <http://commons.apache.org/proper/commons-math/userguide/ml.html>.

A proposal for software development management aided by virtualized kanban board.

Proposta para gestão de desenvolvimento de software auxiliado por quadro virtual Kanban.

ALEXANDRE, M. T.; ALMEIDA JR, J. R..*
*Departamento de Engenharia de computação e Sistemas Digitais - Universidade de São Paulo
jorgerady@usp.br, tiago.alexandre@alumni.usp.br

***Abstract*— The Kanban method has been used for several software development companies to expose bottlenecks in their production. The initial Kanban proposal predicts the use of a physical board for controlling and visualizing activities. This proposal suggests the use of a virtual Kanban board to facilitate the managing process due to automatic metrics extraction. To endorse this proposal, approximately two years of data have been gathered from a software development company to verify the people commitment to virtual board usage comparing their actions taken on the virtual board with the actually registered activity in the source code manager software. Therefore, raise some evidence about the efficacy of the virtual Kanban board usage.**

***Keywords*— Kanban, agile methodology, kanban board, virtual kanban board.**

Resumo—*O método Kanban tem sido utilizado para evidenciar gargalos na produção de software em diversas empresas de desenvolvimento. A proposta inicial do Kanban prevê o uso de um quadro físico para controle e visualização das atividades. Esta proposta sugere que o quadro seja construído de maneira virtual para permitir a extração de métricas de maneira automatizada e assim, facilitar o processo de gestão. Para endossar a proposta, foram analisados dados de aproximadamente dois anos de utilização de quadro virtual Kanban em uma empresa de desenvolvimento de software e verificar a aderência das informações apresentadas no quadro em relação ao real estágio de desenvolvimento através da comparação destes dados com os dados obtidos nos controladores de versionamento de código fonte. Assim, levantar evidências sobre a eficácia do uso dos quadros virtuais de Kanban.*

***Palavras-chave*— Kanban, metodologia ágil, quadro kanban, quadro virtual kanban.**
Classificação—Mestrado.
Categoria— Iniciante.

I. INTRODUÇÃO

A crescente complexidade dos sistemas computacionais a serem desenvolvidos gerou inúmeras complicações para os desenvolvedores de software ao longo dos anos. Para lidar com sistemas muito grandes, é bastante comum, a proposta de sua divisão em pequenos componentes. O ato de desenvolver cada componente pode ser representado, por uma tarefa ou atividade. Dessa forma, um sistema é completo quando se completam todas as tarefas que compreendem o seu desenvolvimento.

A natureza dinâmica do desenvolvimento de software, que tem prazos muito apertados e elevado número de mudanças de requisitos, que tem sido os principais motivos das falhas nos projetos nas últimas décadas [1,2], é levada em conta pelo método Kanban que se adequa bem a este tipo de situação [3].

É bastante comum que, após iniciada, uma tarefa permaneça cerca de 85% do tempo em alguma fila. [4] e reduzir o tempo de fila das tarefas é um dos objetivos do método Kanban.

O método Kanban, derivado do Lean, para o gerenciamento de produção de bens "não tangíveis", como software, apresenta o quadro de atividades (Kanban Board) como sendo a principal ferramenta para se conseguir visualizar o fluxo de trabalho de uma determinada organização. Sendo este, o primeiro dos cinco elementos de uma implantação bem-sucedida do método. [5].

Kanban board expõe o fluxo de trabalho o que permite a identificação de gargalos no processo. Assim, é possível estabelecer limites no fluxo o que acelera as entregas e reduz riscos técnicos e de negócios [6].

Devido a diversos fatores como, diversidade de localização física dos membros da equipe e a dificuldade de elaboração de métricas utilizando material não digitalizado, algumas empresas apresentaram propostas para virtualização do quadro (VQ) de atividades tais como LeanKit e Jira.

Uma das características do Kanban é a sua inicial adesão ao processo de trabalho. A VQ pode engessar um pouco esta adesão devido a restrições inerentes da ferramenta.

Além disso, quadros virtuais podem tornar as reuniões diárias de acompanhamento um pouco diferentes em relação ao modelo proposto por Anderson em frente ao quadro físico.

O Kanban tem evoluído bastante entre as empresas de desenvolvimento de software. Muitos conceitos estão sendo testados empiricamente e os resultados das experiências estão orientando a evolução do método [3].

O presente trabalho propõe analisar dados de dois anos de acompanhamento de métricas de Kanban em uma empresa de desenvolvimento de software que utilizou quadro virtual durante todo o período. Os dados extraídos da ferramenta de acompanhamento virtual serão cruzados com os dados da ferramenta de versionamento de código.

A técnica do erro quadrático médio [7] será utilizada para avaliar se os dados informados no quadro virtual realmente representam o trabalho gerado efetivamente. O que revela o nível de confiança das informações extraídas da ferramenta. Também foi observado se, apesar de eventuais discrepâncias, pode ter acontecido uma regressão à média durante o período, o que seria uma evidência a favor da comprovação da eficácia do quadro virtual.

O método Kanban conseguiu melhorar a comunicação e auxiliar no desafio de desenvolver software em times globais e a utilização do quadro Kanban foi o principal fator para resolver o problema da comunicação devido às diferenças de fuso horário que dificulta a realização de reuniões presenciais [9].

II. BENEFÍCIOS DO MÉTODO KANBAN

Segundo estudos publicados acerca do uso do método em desenvolvimento de software, os principais benefícios são [10]:

- Redução do tempo de entrega de software;
- Melhoria na qualidade do software entregue;
- Melhoria na comunicação e coordenação;
- Aumento da consistência das entregas;
- Redução do número de defeitos reportados por clientes.

A. Quadro de acompanhamento de atividades

O quadro de acompanhamento de atividades é uma das principais práticas para se adotar o método Kanban. Pois expõe alguns conceitos como limitação do trabalho em progresso e os gargalos do processo conforme mostra a figura 1 [8].

Fig. 1. Quadro Kanban. Adaptado de [8]

B. Quadro virtual de acompanhamento

Com a utilização de software especializados, é possível adaptar o quadro Kanban para o ambiente digital [11]. Isso muda o contexto das reuniões em que cada membro da equipe pode fazer de sua máquina, via ferramentas de comunicação e compartilhamento de tela, permitindo a participação efetiva de pessoas em outras localidades.

Além disso, o fato das ferramentas criarem as medições automaticamente, se bem alimentadas durante as reuniões, espera-se que os gestores possam extrair informações fundamentais sobre o andamento das atividades para tomadas de decisão. O uso de um sistema Kanban hospedado na Web já foi utilizado com sucesso na indústria mecânica e tornou o processo existente mais efetivo pois combinou a simplicidade do método com as capacidades da Web, melhorando a visibilidade, abrangência da aplicação para outras áreas da empresa e medições de performance em tempo real. [11]

III. PROPOSTA

Este artigo propõe a substituição do quadro Kanban físico por um quadro digitalizado para acompanhamento do desenvolvimento de projetos de software tendo os seguintes benefícios como motivação:

- Viabilizar a participação em reuniões diárias dos integrantes que estejam em trabalho remoto;
- Viabilizar o acompanhamento das atividades por integrantes que não compartilham o mesmo ambiente;
- Evitar a perda de informações por eventuais falhas nos papéis autoadesivos;
- Agilizar a geração de métricas baseadas no andamento das tarefas registradas no quadro;
- Reduzir o consumo de materiais de escritórios como papéis autoadesivos, canetas hidrográficas;
- Reduzir o tempo de extração de informações do quadro Kanban para geração de métricas para gestão do projeto.

Um dos grandes argumentos para o uso do quadro físico é de que ele permite que todos os envolvidos no projeto estejam sempre cientes do andamento das atividades e de onde estão os gargalos. Como as reuniões são diárias e o quadro deve ser atualizado nas reuniões, é muito provável que o mesmo se mantenha consistente com real estágio do desenvolvimento [5]

Assim, uma grande preocupação nesta proposta é que o quadro virtual, por não ter uma visibilidade enfática no ambiente de desenvolvimento, possa apresentar defasagens ou inconsistências entre o que foi registrado e o que foi devidamente desenvolvido. Entre os fatores que podem ocasionar estas inconsistências, podemos citar o erro humano e a falta de um sistema automatizado de acompanhamento.

Desse modo, um estudo de caso foi elaborado para comparar as marcações realizadas no quadro virtual com os registros no sistema de versionamento de código para identificar se os registros estavam consistentes e, portanto, confiáveis.

IV. Estudo de Caso

Um grande projeto de desenvolvimento de software de uma empresa do setor de restaurantes foi acompanhado durante dois anos. O projeto agrupou algumas características importantes ao estudo como um quadro digital de Kanban com reuniões diárias via internet sendo alguns membros, eventualmente, em locais diferentes.

O projeto é composto por desenvolvedores experientes e pré-treinados nos padrões de desenvolvimento que compreendem: Mínimo de 95% de cobertura de código por testes unitários, revisão de código por pares, ferramentas automatizadas para padronização de escrita, reuniões diárias de acompanhamento de projeto, sistema de integração contínua com compilação e execução dos testes unitários em servidores corporativos, entregas pequenas e rápidas de 1 a 3 dias em média. Além de um largo conceito de definição de "conclusão" que compreende documentação, verificação de cumprimento de requisitos e critérios de aceitação por uma equipe autônoma de medição de qualidade.

As marcações do andamento das atividades foram extraídas da ferramenta de gestão de projeto, assim como os registros destas mesmas atividades no sistema de versionamento de código.

A comparação de defasagem de data destes registros poderá dar sustentação para a proposta quanto à mitigação do risco de defasagem das informações.

V. Resultados esperados

Ao avaliar as métricas do estudo de caso, espera-se não encontrar discrepâncias significativas entre os registros do quadro virtual e o software de versionamento de código utilizando-se a técnica do erro quadrático médio [7] para comparação. Com isso, concluir que as métricas obtidas durante o estudo de caso realmente refletiram o trabalho dos desenvolvedores e que estes proveram informações seguras para os gestores ao atualizarem manualmente o quadro virtual. Assim, dar uma sustentação experimental para a proposta do uso do quadro virtual para projetos de software que utilizem o método Kanban como base de gestão.

VI. Trabalhos futuros

É possível propor, com auxílio de ferramentas apropriadas, uma solução de integração entre o software de controle de versão e o quadro virtual de controle de atividades de modo que o quadro reflita, obrigatoriamente, o que acontece de fato no desenvolvimento. Desse modo, mitigar o risco do erro humano no registro das atividades.

Referências

[1] BOEHM, B. "Software risk management: Principles and practices," IEEE Software, vol. 8, no. 1, pp. 32–41, 1991.

[2] ADDISON, T. VALLABH S., "Controlling software project risks: An empirical study of methods used by experienced project managers," in Proceedings of the SAICSIT'02. South African Institute for Computer Scientists and Information Technologists, 2002, pp. 128–140.

[3] IKONEN, MARKO, ELENA, P. FABIAN, F. PETRI, K. PEKKA, A. "On the Impact of Kanban on Software Project Work: An Empirical Case Study Investigation." 16th IEEE International Conference on Engineering of Complex Computer Systems (2011): 305-314.

[4] VACANTI, S.D. "Actionable Agile Metrics for Predictability: An Introduction" Inc., Leanpub, Year: 2015.

[5] ANDERSON, D. J. "Kanban: Successful Evolutionary Change for Your Technology Business". Blue Hole Press.Year 2010.

[6] Middleton, P. and Joyce, D. "Lean Software Management: BBC Worldwide Case Study," IEEE Transactions on Engineering Management, vol. 59, no.1, pp. 20-32, Feb. 2012.

[7] LEHMANN, E. L. CASELLA, G. "Theory of Point Estimation" (2nd ed.). New York: Springer. ISBN 0-387-98502-6 Year: 1998.

[8] ANDERSON, D. J., CARMICHAEL, A. "Essential Kanban Condensed" Seattle, Washington. Lean Kanban University. ISBN: 978-0-9845214-2-5. First edition, Year: 2016.

[9] TANNER, M. DAUANE, M "The use of kanban to alleviate collaboration and communication challenges of global software development" Issues Inf. Sci. Inf.Technol., 14 Year: 2017, pp. 177-197

[10] AHMAD, M. O. MARKKULA, J. & OIVO, M. "Kanban in software development: A systematic literature review". 39th Euromicro Conference on Software Engineering and Advanced Applications, 9–16. http://doi.org/10.1109/SEAA.2013.28 Year: 2013.

[11] WAN, H. CHEN, F. F. "A Web-based Kanban system for job dispatching, tracking, and performance monitoring". Int J Adv Manuf Technol 38: 995. Year: 2008

Automatic Safety Test Generation for Railway signaling and communication system

Santos, I. J; Vismari, L. F.; Camargo, J. B.
Safety Analysis Group, School of Engineering, University of São Paulo, São Paulo
E-mail: ivanildo_jacintho@usp.br

***Abstract*—The interlocking (ILK) is responsible for controls points, signals, and locks with routes to work safely and prevent conflicts, derailments, and any unsafe condition. It is necessary to ensure the safety at ILK control, validation is usually realized by tests. However the tests have some limitations, it is not scalable, the tests are too long, and can not guarantee the full coverage of the logic. Automatic tests generation are a possible solution for this kind of limitation, given the power to generate a large number of test cases and process it. Guided by a SLR (systematic literature review), we discuss some approaches relevant to this problem, vantages disadvantages and problems by then. To compare results and differences about each approach we apply it in a simulated use case, a logic code of a vital segment. As conclusion we compared some approaches using formal methods, which has the same problem in large systems lead with search space, processing time and the safety properties.**

***Keywords*— Automatic test generation; formal methods, interlocking system, safety.**

***Classification*— Master's Degree**

***Category*— Beginner**

I. Introduction

Safety is considered essential in critical systems like airplanes, railways, nuclear systems and others which represents dangers to life and environment. In railway domain, the interlocking is responsible by the safety movements at the train, interacting with signaling, track segment, and points. To guarantee the safety the control needs to be verified. In EU (European Union) railways [1] in 2016 was reported 1762 accidents, most of then collisions and derailments, 946 resulting in death. Thinking about how to prevent this problem, tests could be a possible solution, the system has to work without unacceptable safety risks when It has a failure. So the maximum number of conditions have to be tested, conditions which represent real cases. The manual test is used by industry to It, simulating different real situations, but it could be better and scalable when applied an automatic test generation. The difference of common generation which has an infinite number of inputs and outputs as alphanumeric or numbers, that system is boolean based. The interlocking systems before built with physical relays which were programmable locally and occupated much space is now implemented with Programmable Logic Controller (PLC), and use a boolean logic, similar with the relay logic but more accessible and editable, which directs the problem to a test of satisfiability. For this problem formal methods approaches are the most used in to test generation as [2],[3]. But it also has some problems in a large-scale system the search space as time execution is a problem which needs optimization, and the safe properties or models usually make manually. Guided by a SLR, a technique to put together the bests publications with low bias [4], we define the state-of-art and compare some approaches thinking on our real case.

II. Railway Interlocking System

The railway system can be divided into yards where the train operates, and stations and the equipment are divided in Vital and non-vital, the first is equipment's which failure can impact in unsafe state, the non-vital is where there is not this risk.

Interlocking Railway system is responsible by the work of railway without collision conflict or accidents. The implementation studied by this research works with computer based interlocking, where a PLC use ladder logic, based on relay logic. Ladder logic is considered a representative sequence of boolean operations [2]. As the example the boolean expression $z := (w \bigwedge \neg x) \bigvee y$ is represented in ladder by the figure 1 :

Fig. 1. Ladder example

Here logic is linear, verifying the inputs of each variable (w,x,y), and if these conditions are satisfied the out (z) is activated, line per line until all steps finished. Between the components controlled by the ILK as Boolean variable are:

Track Segments. Train lines are divided into segments, and each segment has a circuit responsible for monitoring the track occupation [2].

Signals. the most common inform how the train has proceeded, stop or decelerate by position of trains.

Points or switches. The responsible to merge two lines into one line, or change the train track, this has two possible states reverse and normal, in normal the train follow in your actual track in reverse it changes to another track,

Routes. created by control tables, are composed of tracks segments creating a path to the train, passing by points and signals when necessary.

The main focus is on movement equation, a sequence of boolean conditions which has to be satisfied to proceed using the components as variables.

III. Methodology

Following the SLR methodology, we define some research questions which guide the research with the objective to discuss the state-of-art about automatic test generation. The following questions :

- RQ1 - How the signaling and interlocking system works?
- RQ2 - What problems and challenges for test automation?
- RQ3 - What exists to ladder logic test generation?
- RQ4 - What the state-of-art for test generation of ILK?
- RQ5 - What the completeness at ILK with test generation?
- RQ6 - How guarantee the validity in a test of ILK?
- RQ7 - What is the mean of execution time of manual test against the automatic test?

Based on this questions, we define the keywords, and for then we define the strings searches, looking in the well-knowledge databases IEEE Xplorer, science direct, Scopus and springer, at period of 2009 to 2018, with the objective to take the last studies including implementations around the world We define five search strings:

- S1 - Interlocking system test case generation
- S2 - Automated test Interlocking system
- S3 - Test case generation ladder based
- S4 - Test case generation Boolean based
- S5 - Validation of Interlocking Systems

As result at strings in databases, we have the table I which represents the first results in each database.

Strings	IEEExplore	Science Direct	Scopus	Springer
S1	5	1	15	778
S2	7	8	3	379
S3	2	1	7	655
S4	22	6	43	2256
S5	23	30	58	454

TABLE I
FIRSTS RESULTS.

In the first three databases the search was focused on Title, keywords, and resume (TAK), at least there is not filter TAK, the Springer Link does not have this option, which explain the big number of results.

As expected the result was too large, so it is necessary to create some selection criteria we define 7 exclusion criteria and 4 inclusion criteria after applying these criteria we have the table II with results after exclusion and inclusion criteria:

Exclusion Criteria: EC1: Papers written in english or portuguese. EC2: Papers with not available the full-text. EC3: Papers not related to Tests Generation. EC4: Papers not related to safety. EC5: Papers which not discuss results.EC6: Papers which results are not reproducible. EC7: Papers in more the one database.

Inclusion Criteria: IC1: Papers with methodology applied is valid, with adequate literature review, and empiric tests well defined. IC2: Papers with tests in practice cases, mainly in Railway Systems. IC3: Papers with optimization techniques. IC4: Papers which presents methodologies in the abstract.

Database	First Results	After EC1-EC8	After IC1IC4
IEEE Xplore	59	32	7
Scopus	46	39	12
Science Direct	126	90	22
Springer Link	4522	189	18
Total	4753	350	59

TABLE II
RESULTS AFTER CRITERIA.

Based on this results we can classify the publications scoring then by 5 quality questions,any question has points of 0 to 10 and the final score is the mean of that, as result we have 42 publications, we also get 4 publications cited in the papers selected, resulting in 46 publications. Classifying this results by the method to solve the problem we have about 4 categories to answer the main questions about the solutions and state-of-art on table III.

Methodology	Authors
Theorem Proving	[5], [6], [7], [8], [3] [9], [2], [10], [11],[12], [13], [14], [15]
Model Checker	[16], [17], [18], [19], [20],[21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32]
Statical Method	[33], [34]
Others	[35], [36], [37], [38], [39], [40], [41], [42], [43], [44]

TABLE III
FINAL REFERENCES.

Model Checker and Theorem proving are the stabilized branches of Formal Methods, this are methods to formalize the problem mathematically and solve this by logic [45]. Model checker basically is a technique which given a model of a system and a logic property, verify systematically if the property holds in that model, the model could be passed as a finite state machine (FSM), UML, conjunctive normal forms (CNF), etc, theorem proving tests if an implementation satisfies a specification, both represented by Boolean formulas.

Statical model cannot be classified like formal methods, because this uses static methods to test some properties of logic as example [34] Monte Carlo method, for estimating the probability (logic) of satisfying a property ψ (safety property). The principle is to generate N random simulations, and to compute the following estimation of . Others are publications for fundamentals or concepts used to answer the questions as RQ1, RQ2, RQ6. The others In formal methods techniques, test generation starts with the creation of safety properties, safety conditions for the work, this is a problem discussed by [2], [3], [29] and others, they solve this problem manually, a safety property can be represented as an invariant, a condition of real system that represents that is opposite of the normal behavior, an example is the command of one point to normal and reverse at same time, it is an invariant, an essential unsafe condition represented by:

$$Points := [normal \bigwedge reverse] \quad (1)$$

If logic tested satisfy this condition in some moment, it is indicate a unsafe condition, a counter-example. So the essentials principles can be defined, which need to be specified looking for variables. By that, the authors can verify the logic by using a model-checker tool (UPPAAL, NUSMV, SPIN) or a theorem proving tool (SAT SOLVER, SMT SOLVER, EVENT-B), if a model used the logic has to be translated for each approach, the same methods are applied in ladder logic for industry with more use of model-checkers. The results of SLR enable us reunion the most used techniques, to test the performance and applicability to our use case, and find better results with low bias.

IV. Use Case

Our use case is a simulated logic of Vital track which contains 654 equations and 272 variables, this logic is expressed by a file .ERQ generated by the PLC, which contains the ladder equations. In some systems logic is tested manually by the test specialists using a simulation tool as VITAL SIM or PLCs simulators, but it takes too long time to guarantee the better coverage in little modifications as well as creating new logic. The simulation tool generates a translated logic to a formal language. Our implementation, thinking in real systems, will consist in use the movement equations translated to a model, and combining then to safety properties, created by a method suggested by [34] which define the formal properties based on the real topology of the track using the RaiMl a language to describe it and python to interpret this topology, then extract the properties based on essential knowledge, as inputs which are used by the formal method tools to find used as figure 2 shows:

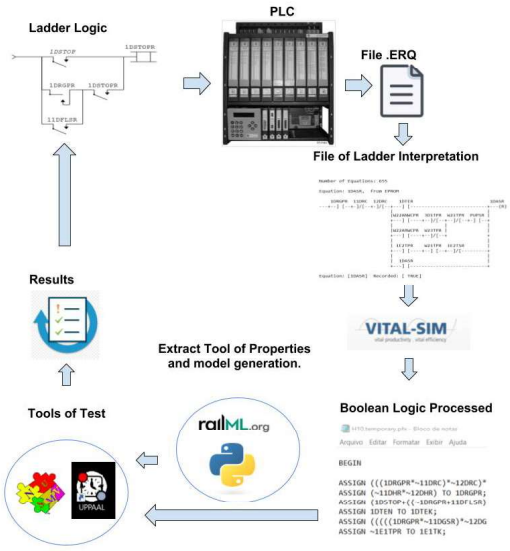


Fig. 2. Proposed Flow.

As result we hope to find the counter-examples for each property, and as the flow by that, the ladder logic can be modified, so the cycle restart. To test the capability to getting unsafe conditions will be injected at least 3 unsafe conditions in logic to be tested, at each approach experimented. The conditions will be inputs in at least 3 essential principles. A possibility to command two routes which have the same segment; A possibility to train follow a track occupied; A possibility to command points in different positions at same time.

We will verify the time execution, number of tests, and if it gets by the technique.

V. Conclusion

As conclusion of SLR we can observe the behavior of two methods Theorem Proving and Model Checker in use of different tools, we validate the MiniSAT, NuSMV, UPPAAL in a simple test of functionalities give by the developers of each tool, to evaluate the difficulty of implementation and usability. To our use case, MiniSat is not applicable, because this is not scalable, and is not hard to interpret, to use MiniSat the Logic has to be translated to CNF [9], this form use only number to represent variables which difficult implementation for this use case. NuSMV is really applicable for our problem, It is easy to understand by logic and widely used in interlocking tests, It verifies all possibilities in model to ensure the property is accomplished, It has some libraries to optimization and has good performance. UPPAAL is the most visual tool to execute the tests, but as the CNF the model has to be translated, redrawn in your tool like a network timed automata [17], it works like a simulator over the time, and verify the safety properties. The gain of test generation is discussed by [19], using a SAT-based applied on European Railway Traffic Management, the automatic generation is 42% inferior in time and superior in number of tests executed against manual tests, improving the coverage. The problems found was mainly these properties generations and lead with problem of large-scale systems as the same in [33] the gain is about 20%. The next steps are the tests implementation on our use case, where is expected similar results with the literature, and again of 20%.

VI. Future Work

As future works we will do the tests in a large-scale ILK system, implementing an optimization method for it, Once time consuming and processing is long, as [10] and [29] suggest optimization for large-scale systems, as miStrategy.

Acknowledgment

The authors are grateful to VALE S.A. to financial and technical support to this research.

References

[1] Eurostat. Railway safety statistics. *Departmet for transport*, n. November 2016, p. 2016–2018, 2016.

[2] KANSO, K.; MOLLER, F.; SETZER, A. Automated Verification of Signalling Principles in Railway Interlocking Systems. *Electronic Notes in Theoretical Computer Science*, v. 250, n. 2, p. 19–31, 9 2009. ISSN 15710661.

[3] GHOSH, S. et al. Formal Methods for Validation and Test Point Prioritization in Railway Signaling Logic. *IEEE Transactions on Intelligent Transportation Systems*, v. 18, n. 3, p. 678–689, 3 2017. ISSN 1524-9050.

[4] SIDDAWAY, A. What is a systematic literature review and how do I do one? *University of Stirling*, n. Ii, p. 1–13, 2014. ISSN 15269523.

[5] B, A. B. et al. *Software Engineering and Formal Methods*. Cham: Springer International Publishing, 2014. v. 8368. 237–251 p. (Lecture Notes in Computer Science, v. 8368). ISBN 978-3-319-05031-7.

[6] B, L. H. V.; HAXTHAUSEN, A. E.; PELESKA, J. Formal Modeling and Verification of Interlocking Systems Featuring Sequential Release. v. 1, p. 223–238, 2015.

[7] DAVE, M.; AGRAWAL, R. Search based techniques and mutation analysis in automatic test case generation: A survey. *2015 IEEE International Advance Computing Conference (IACC)*, p. 795–799, 2015.

[8] FÜRST, A. et al. Large-scale system development using Abstract Data Types and refinement. *Science of Computer Programming*, Elsevier B.V., v. 131, p. 59–75, 2016. ISSN 01676423. Disponível em: <http://dx.doi.org/10.1016/j.scico.2016.04.010>.

[9] JAMES, P. SAT-based Model Checking and its applications to Train Control Systems. n. February, 2010.

[10] LI, Z. et al. Automatic test generation of large boolean expressions in Computer Based Interlocking System. 2017.

[11] PILL, I.; WOTAWA, F. Automated generation of (F)LTL oracles for testing and debugging. *Journal of Systems and Software*, Elsevier Inc., v. 139, p. 124–141, 2018. ISSN 01641212.

[12] SONG, J.; JEE, E.; BAE, D.-H. FBDTester 2.0: Automated test sequence generation for FBD programs with internal memory states. *Science of Computer Programming*, v. 163, p. 115–137, 2018. Disponível em: <www.elsevier.com/locate/scico>.

[13] STANKAITIS, P.; ILIASOV, A. Safety Verification of Modern Railway Signalling with the SafeCap Platform. p. 1–4, 2017.

[14] VU, L. H.; HAXTHAUSEN, A. E.; PELESKA, J. Formal modelling and verification of interlocking systems featuring sequential release. *Science of Computer Programming*, Elsevier B.V., v. 133, p. 91–115, 2017. ISSN 01676423. Disponível em: <http://dx.doi.org/10.1016/j.scico.2016.05.010>.

[15] MOLNÁR, B.; ERCSEY-RAVASZ, M. Asymmetric Continuous-Time Neural Networks without Local Traps for Solving Constraint Satisfaction Problems. *PLoS ONE*, v. 8, n. 9, p. 3–4, 2013. ISSN 19326203.

[16] OLIVEIRA, K. D. V. et al. Automatic timed automata extraction from ladder programs for model-based analysis of control systems. *IEEE International Symposium on Industrial Electronics*, p. 90–95, 2010.

[17] GHOSH, S. et al. Formal verification of movement authorities in automatic train control systems. *IET Conference Publications*, v. 2016, 2016.

[18] ANGELETTI, D. et al. Automatic test generation for coverage analysis of ERTMS software. In: *Proceedings - 2nd International Conference on Software Testing, Verification, and Validation, ICST 2009*. [S.l.: s.n.], 2009. p. 303–306. ISBN 9780769536019. ISSN 03029743.

[19] ANGELETTI, D. et al. Using bounded model checking for coverage analysis of safety-critical software in an industrial setting. *Journal of Automated Reasoning*, v. 45, n. 4, p. 397–414, 2010. ISSN 01687433.

[20] B, Q. C.; SCHAUS, P. A Dedicated Algorithm for Verification of Interlocking Systems. In: SKAVHAUG, A.; GUIOCHET, J.; BITSCH, F. (Ed.). *35th International Conference, SAFECOMP 2016 Trondheim, Norway, September 2123, 2016 Proceedings*. Cham: Springer International Publishing, 2016. (Lecture Notes in Computer Science, v. 9922), p. 76–87. ISBN 978-3-319-45476-4.

[21] BONACCHI, A. et al. Validation process for railway interlocking systems. *Science of Computer Programming*, Elsevier B.V., v. 128, p. 2–21, 2016. ISSN 01676423.

[22] DINCEL, E.; ERIS, O.; KURTULAN, S. Automata-based railway signaling and interlocking system design. *IEEE Antennas and Propagation Magazine*, v. 55, n. 4, p. 308–319, 2013. ISSN 10459243.

[23] ENOIU, E. P. et al. Automated test generation using model checking: an industrial evaluation. *International Journal on Software Tools for Technology Transfer*, v. 18, n. 3, p. 335–353, 2016. ISSN 14332787.

[24] JAMES, P. et al. Verification of Solid State Interlocking Programs. In: . [S.l.: s.n.], 2014. v. 8368, p. 253–268. ISBN 978-3-319-05031-7.

[25] Jidong Lv et al. A model-based test case generation method for function testing of Train Control Systems. *2016 IEEE International Conference on Intelligent Rail Transportation (ICIRT)*, v. 3, p. 334–346, 2016.

[26] HAXTHAUSEN, A. E.; BLIGUET, M. L.; KJAER, A. A. Modelling and verification of relay interlocking systems. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. [s.n.], 2010. v. 6028 LNCS, p. 141–153. ISBN 3642125654. ISSN 03029743. Disponível em: <http://link.springer.com/10.1007/978-3-642-12566-9$_{8}$¿.

[27] LV, J. et al. Model-based test case generation for function testing of CTCS-3 onboard subsystem. *International Journal of Control and Automation*, v. 8, n. 10, p. 171–178, 2015. ISSN 20054297.

[28] MANI, P.; PRASANNA, M. Automatic test case generation for programmable logic controller using function block diagram. *2016 International Conference on Information Communication and Embedded Systems (ICICES)*, p. 1–4, 2016.

[29] BUSARD, S. et al. Verification of railway interlocking systems. *Electronic Proceedings in Theoretical Computer Science*, v. 184, p. 19–31, 6 2015. ISSN 2075-2180. Disponível em: <http://lvl.info.ucl.ac.be http://arxiv.org/abs/1506.03554>.

[30] WU, Y. C.; FAN, C. F. Automatic test case generation for structural testing of function block diagrams. *Information and Software Technology*, v. 56, n. 10, p. 1360–1376, 2014. ISSN 09505849.

[31] GONSCHOREK, T.; ORTMEIER, F. Bringing formal methods on the rail: On automatic verifying railroad interlockings from railML models ForMOSA View project. In: *Safety and Reliability Safe Societies in a Changing World* . [S.l.: s.n.], 2018.

[32] HAXTHAUSEN, A. E. Automated generation of formal safety conditions from railway interlocking tables. *International Journal on Software Tools for Technology Transfer*, v. 16, n. 6, p. 713–726, 2014. ISSN 14332787.

[33] CAPPART, Q. Verification of Railway Interlocking Systems and Optimisation of Railway Traffic. n. December, 2017.

[34] CAPPART, Q. et al. Verification of Interlocking Systems Using Statistical Model Checking. In: *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*. [S.l.]: IEEE, 2017. p. 61–68. ISBN 978-1-5090-4636-2.

[35] BRKIĆ, R.; ADAMOVIĆ, Z. Research of defects that are related with reliability and safety of railway transport system. *Russian Journal of Nondestructive Testing*, v. 47, n. 6, p. 420–429, 2011. ISSN 1061-8309.

[36] FANTECHI, A.; FLAMMINI, F.; GNESI, S. Formal methods for railway control systems. *International Journal on Software Tools for Technology Transfer*, v. 16, n. 6, p. 643–646, 2014. ISSN 14332787.

[37] GURNÍK, P. Next Generation Train Control (NGTC): More Effective Railways through the Convergence of Main-line and Urban Train Control Systems. *Transportation Research Procedia*, v. 14, p. 1855–1864, 2016. ISSN 23521465.

[38] KIM, J. et al. Cold performance of various biodiesel fuel blends at low temperature. *International Journal of ...*, v. 13, n. 2, p. 293–300, 2012. ISSN 1229-9138.

[39] MAJMA, N.; BABAMIR, S. Software test case generation & test oracle design using neural network. *22nd Iranian Conference on Electrical Engineering, ICEE 2014*, n. Icee, p. 1168–1173, 2014.

[40] MARAIS, J.; BEUGIN, J.; BERBINEAU, M. A Survey of GNSS-Based Research and Developments for the European Railway Signaling. *IEEE Transactions on Intelligent Transportation Systems*, v. 18, n. 10, p. 2602–2618, 2017. ISSN 15249050.

[41] SUN, P.; COLLART-DUTILLEUL, S.; BON, P. A model pattern of railway interlocking system by Petri nets. *2015 International Conference on Models and Technologies for Intelligent Transportation Systems, MT-ITS 2015*, n. June, p. 442–449, 2015.

[42] TSENG, W.-H.; FAN, C.-F. Systematic scenario test case generation for nuclear safety systems. *Information and Software Technology*, v. 55, n. 2, p. 344–356, 2013. ISSN 09505849. Disponível em: <http://linkinghub.elsevier.com/retrieve/pii/S0950584912001838>.

[43] YIN, J. et al. Research and development of automatic train operation for railway transportation systems: A survey. *Transportation Research Part C: Emerging Technologies*, v. 85, p. 548–572, 2017. ISSN 0968090X.

[44] YONG, Z.; ZHIBIN, P.; CHUNGUI, Y. Research on the Method and Tool for Automatic Generation of Application Data for Interlocking Simulation System. In: *2011 International Conference on Control, Automation and Systems Engineering (CASE)*. [S.l.]: IEEE, 2011. p. 3–6. ISBN 9781457708602.

[45] CLARKE, E. M. et al. Formal methods: state of the art and future directions. *ACM Computing Surveys*, v. 28, n. 4, p. 626–643, 1996. ISSN 03600300.

Multi-agent Simulation of Unmanned Air Vehicles Using Netlogo
Simulação Multiagentes de Veículos Aéreos Não Tripulados Usando Netlogo

FERRARE, F. D.*; CUGNASCA, P. S.*
*Escola Politécnica - Universidade de São Paulo (USP)
E-mail: {felipe.ferrare,cugnasca}@usp.br

***Abstract*—Unmanaged Air vehicles (UAVs) are now part of our society. However the great number of vehicles sharing the same airspace, create risk and security concerns. To optimize the trajectories and the airspace capacity we can use computational simulation tools, then using multi-agent systems (MAS) we can simulate the behavior of multiple UAVs and use their collective intelligence to get better results. In this work will be used a simulation model (2D and 3D) using the programming language Netlogo to validate the security and the trajectories quality in a specific scenario.**

***Keywords*— Unmanned Air Vehicles; Air Traffic control; Multi-Agent; Simulation; Safety.**

***Resumo*— Veículos aéreos autônomos (VANTs) estão cada vez mais difundidos na nossa sociedade. Mas a grande quantidade de veículos dividindo o mesmo espaço aéreo, cria riscos e problemas de segurança. Para podermos otimizar trajetórias e a capacidade do espaço aéreo podemos usar de simulações computacionais, assim usando os sistemas multiagentes (SMA) podemos simular o comportamento de múltiplos VANTs nos aproveitar de sua inteligência coletiva para obter resultados melhores. Nesse trabalho será usado um modelo de simulação (2D e 3D) usando a linguagem Netlogo para validar a segurança e qualidade de trajetórias em um cenário específico.**

***Palavras-chave*— Veículo aéreo não tripulado; Controle de Tráfego aéreo; Multiagentes; Simulação; Segurança.**

***Classificação*— Mestrado**

***Categoria*— Iniciante**

I. Introdução

O Objetivo desse trabalho é analisar a performance de diferentes tipos de algoritmos em um ambiente usando sistemas multiagentes (*multi-agent system* - MAS) para otimização das trajetórias de múltiplos veículos aéreos não tripulados (*unmanaged aerial vehicles* - UAVs).

Verificando assim a segurança e performance de acordo com o aumento de aeronaves no espaço aéreo e principalmente tentando comparar o desempenho entre os diferentes casos.

II. Revisão de Literatura

Seguindo o modelo multicamadas em Beard [1] para o controle de trajetórias em uma aeronave, ele divide em 5 níveis (*aircraft*, *autopilot*, *path following*, *path manager*, *path planner*), com isso podemos ver que que o problema é muito complexo, mas as abordagens existentes na literatura tratam de diferentes níveis, sendo os três primeiros mais ligados ao hardware e os dois últimos ao software puro (parte computacional). Esse trabalho tem como desenvolver algoritmos para trabalhar no nível de *path planner* procurando validar a criação de trajetórias em um cenário complexo.

Algumas abordagens como [2] vão focar na parte computacional usando simulação de alto-nível. Outras abordagens vão focar em uma abordagem de baixo-nível focando nos primeiros componentes, usando ambientes de simulação realistas ou protótipos como em [3].Esse artigo usa uma abordagem de alto nível.

Um agente é uma entidade capaz de agir sobre um ambiente, é caracterizado pelos princípios de autonomia, proatividade, reatividade e habilidade social [4]. Um MAS é um sistema em que se busca analisar o comportamento de múltiplos agentes agindo sobre um mesmo ambiente e interagindo entre si, podendo criar soluções colaborativas melhores que as individuais [5]. Esse trabalho usa de agentes reativos que são um tipo de agente não-colaborativo que apenas reage as informações do ambiente [5].

O uso de agentes reativos foi escolhido por causa de sua simplicidade de implementação, criando a possibilidade de validar os cenários e suposições iniciais em uma primeira fase de simulação, alem disso seu comportamento se assemelha ao comportamento não colaborativo encontrado nos sistemas de UAS atualmente em uso.

Existem vários trabalhos buscando a otimização da trajetória de UAVs, alguns como [2] focam na trajetória de apenas um indivíduo e obstáculos no ambiente. Outros como [6] e [7] focam na colaboração entre os agentes usando métodos de otimização como o *particle swarm-optimization* (PSO) para gerar resultados ótimos e reduzir o número de colisões.

III. Ferramentas

Netlogo é uma linguagem derivada do Logo usada para execução de simulação de MAS; é muito usada por ser simples de usar e oferecer diversos recursos [8]. Ela tem sido usada em simulações de várias áreas como ciências sociais, filosofia e física e tendo muitos trabalhos desenvolvidos usando a

ferramenta, além de servir para validar modelos e hipóteses [9]. Possui aplicações na área de aviação, possuindo na sua biblioteca de exemplos um modelo de simulação 3D de "aterrissagem de aeronave" [10].

Para essas simulações foi usado o ambiente do Netlogo versão 6. As execuções ocorreram em um notebook padrão.

IV. Modelo Desenvolvido

Foram desenvolvidas duas simulações no ambiente Netlogo, ambas descrevendo o mesmo cenário, uma usa um ambiente de duas dimensões (2D) e a outra um ambiente de três dimensões (3D).

No ambiente de desenvolvimento do Netlogo as simulação são construídas em um espaço virtual, um quadrado (ou um cubo), composto de quadrados menores chamados de *patchs*, nesse trabalho esse tamanho de um *patch* menor unidade possível sera considerado como sendo uma unidade de espaço. As simulações operaram em turnos sendo que cada turno corresponde a um *tick*, nesse trabalho consideremos um *tick* como sendo a unidade de tempo padrão.

A figura 1 mostra um diagrama do cenário ambiente 2D, o mundo é um quadrado de lado 32 (no caso 3D um cubo de lado 32). Esse mundo é dividido em quadro partes, em cada parte são colocados inicialmente N veículos aleatoriamente em cada parte, esses veículos são da mesma cor e tem o mesmo objetivo alcançar um ponto no quadrante diagonalmente oposto. Assim todos as aeronaves em um caminho ótimo acabam se cruzando no centro, sendo um cenário simples para gerar o maior número possível de conflitos.

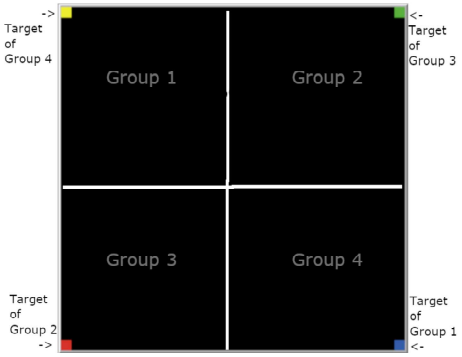


Fig. 1: Mapa do mundo 2D dividido.

Podemos ver em 2 um exemplo da execução no ambiente 2D, e em 3 um exemplo da execução no ambiente 3D.

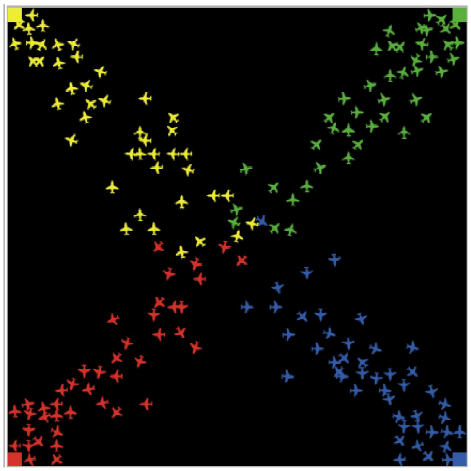


Fig. 2: Visualização 2D da simulação.

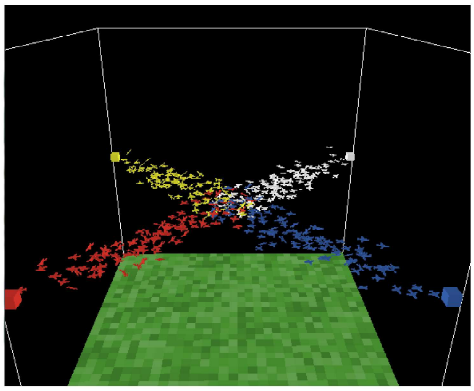


Fig. 3: Visualização 3D da simulação.

Todos as aeronaves são quadricópteros, eles possuem uma frente, mas eles podem se mover para qualquer direção, e no caso 3D podem subir ou descer em ângulos de 35 graus. Assim foi usado um modelo de espaço aéreo em que se tem voo livre (*free flight*) em baixas altitudes, em que a aeronave pode seguir qualquer caminho, diferente de um espaço regulado com corredores aéreos, visando a simulação de um espaço aéreo de baixa altitude, com regras fracas usado somente por UAVs.

Foram feitas simulações variando N (número de aeronaves por grupo), usando 1, 15, 50 e 100. Para eliminar diferenças significativas, já que a simulação possui uma configuração inicial aleatória, cada caso foi executado 300 vezes e foi usada a média de todas essas execuções.

São considerados dois algoritmos:

- Algoritmo 1 - Trajetória aleatória - Com desvio
- Algoritmo 2 - Trajetória Distância euclidiana

O Algoritmo 1 (A1) todas as aeronaves seguem um caminho aleatório, elas podem virar para a esquerda ou direita 35 graus (50% de chance cada) e andar 1 unidade de espaço dentro de uma unidade de tempo (*tick*). No caso da versão 3D ele tambem tem uma chance de subir ou descer (35 graus para cima ou para baixo com 50% de chance cada).

Ele também é capaz de ver o caminho à frente de maneira limitada (1 unidade de espaço) e caso tenha um obstáculo no destino ele pode decidir por ficar parado por uma unidade de tempo.

O Algoritmo 2 (A2) visa encontrar o caminho mínimo local ele usa a formula da distância euclidiana entre o ponto atual e o ponto de destino (conforme equação 1) visando traçar o caminho mais curto entre os dois pontos. Ele também é capaz de detectar quais caminhos estão sendo ocupados (assim como A1), assim clc clabora uma lista dc mclhorcs rotas, selecionando a mais melhor disponível (ou ficando parado caso não exista nenhuma rota segura disponível).

$$V_{\text{Path}} = \sqrt{(X_{\text{Objetive}} - X_{\text{Planed}})^2 + (Y_{\text{Objetive}} - Y_{\text{Planed}})^2} \quad (1)$$

Para mensurar as execuções foi medido o tempo total (*ticks*) média para todos os aviões concluírem e a distância média percorrida por todos os aviões por execução. Tentando comparar as execuções foi feita a equação 2), que faz uma razão entre a distância e tempo (como no máximo ele pode andar uma unidade de tempo por espaço, esse número é uma fração mcnor do quc 1, sc aproximando dc 1 com uma execução ótima e dc 0 numa execução ruim).

Foram medidos o número total de conflitos, que é a somatória de conflitos durante todo os momentos da execução, sendo que um conflito é duas aeronaves a uma distância de uma unidade de espaço.

$$\frac{T}{\Delta t} = \frac{TrajctoriaMedia}{VarTempo} \quad (2)$$

Colisões ocorrem quando duas aeronaves se encontram no ar no mesmo espaço. Nesse caso ambas as aeronaves são destruídas e se soma ao número total de colisões. A distância percorrida não é considerada.

Podemos ver o código fonte em Netlogo do A1 em 2D na listagem 1 e em 3D na listagem 2. O código do A2 em 3D pode ser visto na listagem 3.

Listagem 1: Algoritmo 1 (2D) (pseudocódigo)

```
função Algoritmo 1 (2D):
direção = DccisãoDircção()
Se(direção == esquerda):
        Vire 35 graus a esquerda
Se(direção == direita):
        Vire 35 graus a direita
Se(Caminho a frente existe e está vazio ):
        Ande 1 Unidade a frente
```

Listagem 2: Algoritmo 1 (3D) (pseudocódigo)

```
função Algoritmo 1 (3D):
direção = DecisãoDireção()
Nível = DecisãoNivel()
Se(direção == esquerda):
        Vire 35 graus a esquerda
Se(direção == direita):
        Vire 35 graus a direita
Se(Nível == Cima):
        Vire 35 graus para cima
Se(Nível == Baixo):
        Vire 35 graus para baixo
Se(Caminho a frente existe e está vazio ):
        Ande 1 Unidade a frente
```

Listagem 3: Algoritmo 2 (3D) (pseudocódigo)

```
Função Algoritimo 2 (3D):
Para Todos
os ângulos de subida (0, −35, 35):
Para todos
os ângulos de virada (0 45 90 135 180
225 270 315):
        Se(Caminho a frente existe
        e está vazio):
                Adicionar a
                Lista dc caminhosVálidos
        Para Todos os CaminhosVálidos:
                Resultado =
DistanciaEuclidianaDestino(Caminho)
        Se(Resultado > Resultado_Otimo):
                Resultado_Otimo = Resultado
                Caminho_Otimo = Caminho
FimPara
FimPara
Se Existe um Caminho_Otimo :
        Executa(Caminho_Otimo)
```

V. Resultados

Os resultados do modelo 2D podem ser vistos do A1 na tabela I e do A2 na tabela II. Os resultados do modelo 3D podem ser vistos do A1 na tabela III e do A2 na tabela IV.

N	Conflitos	Colisões	Trajetória	Δt	T/Δt
1	6386,133	0	641,532	3254,600	0,210
15	180284,523	0,010	1090,009	9420,037	0,119
50	1778381,730	1,170	2733,730	21209,973	0,119
100	11202562,090	12,843	6628,563	51790,183	0,128

Tabela I: Algoritmo 1 - Resultados aleatório 2D (média)

N	Conflitos	Colisões	Trajctória	Δt	T/Δt
1	148,620	0	37,155	42,030	0,885
15	2595,203	0	42,938	54,800	0,784
50	14359,503	0	63,779	100,190	0,637
100	47496,273	0,073	89,978	175,343	0,513

Tabela II: Algoritmo 2 - Resultados Distancia euclidiana 2D (média)

N	Conflitos	Colisões	Trajetória	Δt	T/Δt
1	38539,253	2,877	6206,128	20229,563	0,333
15	564612,960	44,483	7794,578	43720,887	0,189
50	1873996,380	148,237	7870,449	54698,690	0,149
100	3770929,437	296,917	7814,063	60313,257	0,134

Tabela III: Algoritmo 1 - Resultados aleatório 3D (média)

N	Conflitos	Colisões	Trajetória	Δt	$T/\Delta t$
1	154,763	0	38,691	43,870	0,883
15	2415,960	0	40,266	49,790	0,809
50	8930,067	0	44,638	66,950	0,682
100	23180,410	0	56,808	108,203	0,526

Tabela IV: Algoritmo 2 - Resultados Distancia euclidiana 3D (média)

VI. Conclusões

Podemos ver que o número de conflitos e colisões aumentam de acordo com o número de aeronaves ocupando o espaço aéreo. O A1 que tinha como base de seu funcionamento o espaço de busca usado, teve um desempenho muito pior no modelo 3D que no 2D, quanto a colisões e conflitos, apesar de manter a mesma razão de tempo/distância.

Já no A2 teve um desempenho bem parecido na razão (trajetória/Tempo) apesar do 3D ter um tempo mais reduzido, como a abordagem considerada é individualista todos as aeronaves tentam seguir a mesma linha reta congestionando o espaço, e com isso é perdido muito tempo, por isso apesar de tentar criar rotas ótimas individuais, globalmente o resultado é não é ótimo, apesar de ainda ser melhor e mais seguro que a situação aleatória.

Podemos ver que a simulação 2D estar mais longe do cenário real que a 3D ela ainda é útil para se obter informações do modelo proposto.

Como trabalhos futuros recomenda-se obter e testar novos modelos que sejam mais seguros, tenham garantias de serem isentos de colisão. Criação de algoritmos de planejamento que tenham o tempo com uma dimensão (4D) e com isso possam fazer inferências de posições futuras. Além disso validar o desenvolvimento de MAS colaborativos em que exista um planejamento coordenado entre as aeronaves visando a melhoria da performance total do sistema, visando a criação de novos sistemas de UAS mais inteligentes. Focando não só na camada de *path planner*, mas avançando na camada de *path manager* gerenciando as múltiplos conflitos e trajetórias.

References

[1] BEARD R. W.; MCLAIN, T. W. *Small Unmanned aircraft: Theory and Practice*. New Jersey, USA: Princeton University Press, 2012.

[2] LEI, G. et al. Multi-agent path planning for unmanned aerial vehicle based on threats analysis. In: *2011 3rd International Workshop on Intelligent Systems and Applications*. [S.l.: s.n.], 2011. p. 1–4.

[3] BELKADI, A. et al. Distributed path planning for controlling a fleet of uavs : Application to a team of quadrotors. *IFAC-PapersOnLine*, v. 50, n. 1, p. 15983 – 15989, 2017. ISSN 2405-8963. 20th IFAC World Congress. Disponível em: <http://www.sciencedirect.com/science/article/pii/S2405896317325351>.

[4] WOOLDRIDGE, M. *Resoning about Rational Agents*. [S.l.]: The MIT Press, 2000.

[5] WOOLDRIDGE, M. *An Introduction to MultiAgent Systems*. [S.l.]: Wiley Press, 2002.

[6] CHEN, X.; HE, W.; WU, Z. Research of uav's multiple routes planning based on multi-agent particle swarm optimization. In: *2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP)*. [S.l.: s.n.], 2013. p. 765–769.

[7] ALEJO, D. et al. Particle swarm optimization for collision-free 4d trajectory planning in unmanned aerial vehicles. In: *2013 International Conference on Unmanned Aircraft Systems (ICUAS)*. [S.l.: s.n.], 2013. p. 298–307.

[8] WILENSKY, U. *NetLogo*. Northwestern University, Evanston, IL., 1999. Disponível em: <http://ccl.northwestern.edu/netlogo/>.

[9] WILENSKY U.; RAND, W. *An introduction to agent-based modeling: Modeling natural, social and engineered complex systems with NetLogo*. Cambridge, MA: MIT Press, 2015.

[10] WILENSKY, U. *Airplane Landing Example 3D*. Northwestern University, Evanston, IL., 2005. Disponível em: <http://ccl.northwestern.edu/netlogo/models/AirplaneLandingExample3D>.

Glaucoma Diagnosis Using Nerve Fiber Layer Thickness Images
Diagnóstico do Glaucoma Usando Imagens de Espessura da Camada de Fibras Nervosas

BRAGA, Samira J.*; GOMI, Edson S.*
*Escola Politécnica da Universidade de São Paulo

***Abstract*—Glaucoma is a chronic disease characterized by the loss of the nerve fiber layer in the eye. If not treated it can lead to irreversible blindness. Machine learning algorithms can be used to classify glaucoma in eye fundus images, data from OCT or visual field. The goal of this paper is to investigate the possibility of diagnosing glaucoma using images of nerve fiber layer thickness using a convolutional neural network (CNN). Using VGG16 and transfer learning technique, the CNN was trained and used to classify on a dataset of images of nerve fiber layer thickness. Initial results show that the use of OCT images in glaucoma diagnosis is viable. However, high loss on validation dataset suggests overfitting. One hypothesis for this result is the limited number of images in the training dataset.**

***Keywords*— Glaucoma Diagnosis, Optical Coherence Tomography, Convolutional Neural Network, Transfer Learning**

***Resumo*— Glaucoma é uma doença crônica que caracteriza-se pela perda da camada de fibras nervosas no olho. Se não tratada pode levar à cegueira irreversível. Algortimos de aprendizagem de máquina podem ser utilizados para classificar glaucoma em imagens de fundo de olho, dados de OCT ou de campo visual. O objetivo deste trabalho é investigar se é possível fazer o diagnóstico do glaucoma a partir das imagens de espessura da camada de fibras nervosas por meio de uma rede neural convolucional. Utilizando a rede VGG16 com técnica de transfer learning, foi feito o treinamento e classificação de glaucoma em um dataset de imagens de espessura da camada de fibras nervosas. Resultados iniciais mostram que a utilização de imagens de OCT no diagnóstico de glaucoma é viável, porém, o alto erro no dataset de validação indica overfitting. Uma das hipóteses para o resultado é a pequena quantidade de imagens de treinamento.**

***Palavras-chave*— Diagnóstico de Glaucoma, Tomografia de Coerência Óptica, Redes Neurais Convolucionais**

***Classificação*— Mestrado**

***Categoria*— Iniciante**

I. Introdução

Glaucoma é uma neuropatia óptica crônica de lenta progressão que causa perda de campo visual. Pesquisa realizada por Quigley e Broman mostrou que glaucoma é a segunda maior causa de cegueira no mundo e estimaram que atingirá 79,6 milhões de pessoas até 2020 [1]. O glaucoma caracteriza-se pela perda da camada de fibras nervosas no olho, o que pode causar cegueira se não for tratada corretamente [2]. O dano na camada de fibras nervosas acontece antes de alteração no campo visual do paciente e, por isso, o diagnóstico precoce é um fator importante para evitar a perda da visão [3].

Estudos mostraram ser possível utilizar métodos de aprendizagem de máquina para detectar glaucoma e auxiliar na tomada de decisão do oftalmologista. Os dados utilizados foram imagens de fundo de olho, dados de exame de tomografia de coerência óptica OCT e de campo visual [4]–[8].

Não foi encontrado na literatura a utilização de imagens de espessura da camada de fibras nervosas para classificação de glaucoma. O objetivo deste trabalho é investigar se é possível fazer o diagnóstico a partir das imagens da espessura da camada de fibras nervosas por meio de uma rede neural convolucional.

II. Diagnóstico de Glaucoma

Atualmente, o diagnóstico do glaucoma é feito com uma combinação de exame estrutural, por meio de OCT [9], e exame funcional, por meio da perimetria computadorizada SAP (Standard Automated Perimetry) [10]. Os exames estruturais avaliam a camada de fibras nervosas para identificar alterações na sua espessura e os exames funcionais avaliam o campo visual do paciente em busca de áreas de perda da visão.

O exame OCT utiliza o princípio da interferometria luminosa para medir as espessuras das estruturas intraoculares. Ao realizar uma varredura, o equipamento emite feixes de laser

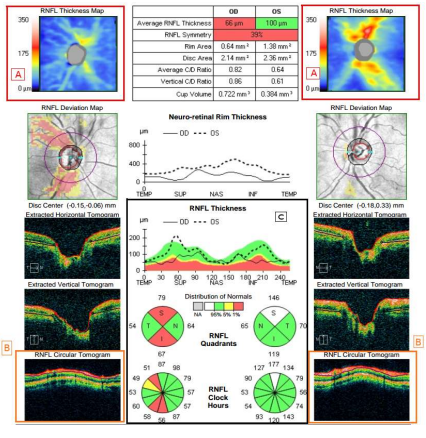


Figura 1. Saída de um exame de OCT.

infravermelho e mede o tempo que a luz leva para ser refletida. Em cada estrutura atravessada, uma parte dessa luz é refletida de volta. O cálculo da espessura é baseado na diferença entre o feixe de luz de referência e a luz refletida [11].

A saída gerada pelo equipamento Cirrus HD-OCT da Carl Zeiss Meditec Inc [12] pode ser vista na figura 1. Na região A estão as imagens de espessuras da camada de fibras nervosas. Essas espessuras são representadas como um mapa de calor, onde espessuras próximas à 0 são apresentadas em azul, do verde ao laranja são espessuras até 175 mícrons e do vermelho ao branco espessuras de 175 à 350 mícrons. O disco central em cinza é a fóvea, ponto cego de onde sai o nervo óptico. Na região B, são exibidas as imagens tomográficas da camada de fibras nervosas em um corte circular em volta da fóvea. A região C exibe gráficos de espessura na região circular ao redor da fóvea, também chamada de mapa TSNIT (Temporal, Superior, Nasal, Inferior, Temporal). Além do gráfico, são exibidos também as médias de espessura por quadrantes e horas de relógio. As medidas de espessuras são comparadas com o banco de dados normativo do aparelho para indicar se a medida está dentro de 95% da população normal (em verde), dentro de apenas 5% da população (em amarelo), ou em apenas 1% da população (em vermelho) [13].

O estudo de Gracitelli *et al.* mostra que os parâmetros de média de espessura por quadrantes e a média global da espessura da camada de fibras nervosas são amplamente utilizados na análise para diagnóstico do glaucoma [4]. No entanto, nenhum exame fornece resultados definitivos da situação do paciente, sendo necessária a avaliação de um profissional oftalmologista especialista em glaucoma para conclusão do resultado. Esta análise não é padronizada e pode variar de acordo com o julgamento do oftalmologista [14].

É possível utilizar classificadores de aprendizagem de máquina para auxiliar na tomada de decisão do oftalmologista. Um classificador de rede neural profunda foi utilizado com dados de exame de campo visual para detectar estágios iniciais de glaucoma [5]. Diferentemente deste estudo, Asaoka *et al.* utilizaram dados do SAP, com uma arquitetura de rede com apenas 4 camadas. Dados de OCT e SAP em conjunto também foram utilizados para treinar diversos tipos de classificadores [6], [7]. Em geral, equipamentos oftalmológicos possuem seus próprios algoritmos para análise e classificação, porém, o estudo de Kwokleung Chan *et al.* mostra que algoritmos de classificação, como *multilayer perceptron*, *support vector machine* e *discriminant analysis*, são mais eficientes [8].

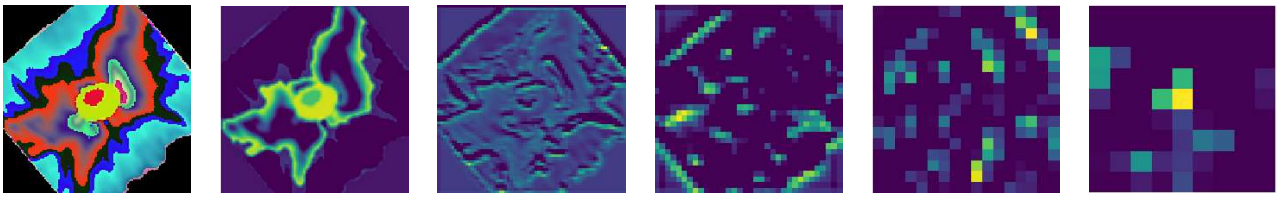
III. Redes neurais convolucionais

Redes neurais profundas estão sendo amplamente utilizadas para classificação e detecção de objetos, principalmente em visão computacional e processamento de linguagem natural. Essas redes consistem em várias camadas conectadas que aprendem a reconhecer padrões nos dados, sejam eles imagens ou sons [15]. O principal tipo de rede utilizado é a rede neural convolucional CNN (Convolutional Neural Network). As CNNs mostraram ser excelentes ferramentas no processamento de imagens, inclusive na área médica, sendo utilizadas para classificação, detecção de objetos e segmentação. Esse sucesso deve-se principalmente à utilização de grandes quantidades de exemplos de treinamento, que permitem que a rede aprenda a reconhecer características a partir dos dados brutos [16].

As CNNs são compostas de várias camadas conectadas, sendo os principais tipos as convolucionais, pooling e as camadas totalmente conectadas. As camadas convolucionais servem como filtros para identificar as características das imagens, como curvas, bordas e cores. As saídas das camadas convolucionais são mapas de características identificadas. A convolução é feita utilizando uma máscara que desliza por todos os pixels da imagem multiplicando os valores do pixel pelos valores da máscara. Essa multiplicação é feita em toda a imagem com diferentes máscaras, gerando as saídas dos diferentes filtros em cada camada de convolução.

Após a identificação dessas características, a camada de pooling as agrupa e reduz a resolução da imagem. Também utilizando uma máscara, a operação de pooling irá calcular o valor máximo em cada região da imagem, agrupando características similares em um mesmo pixel. Na figura 2 é possível acompanhar o agrupamento e a redução da resolução da imagem ao longo de 5 camadas convolucionais e pooling.

As camadas totalmente conectadas recebem todas as características identificadas nas imagens e fazem a classificação final. A saída dessa camada será um vetor com o número de classes a serem classificadas, cada classe terá um valor de probabilidade sendo o maior valor a classe identificada para a imagem. O desenho de uma configuração de uma CNN pode ser vista na figura 3. Várias camadas de convolução e pooling utilizando ativações por ReLU (Rectified Linear Unit)



(a) Imagem de entrada da rede

(b) Imagem de saída da primeira camada convolucional

(c) Imagem de saída da segunda camada convolucional

(d) Imagem de saída da terceira camada convolucional

(e) Imagem de saída da quarta camada convolucional

(f) Imagem de saída da quinta camada convolucional

Figura 2. Exemplos de saídas de cada camada convolucional ao longo da rede.

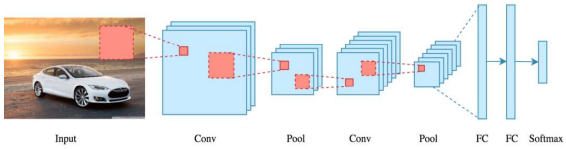


Figura 3. Esquema de camadas de uma rede neural convolucional [18].

são seguidas por duas ou mais camadas totalmente conectadas. O aumento da quantidade de camadas mostrou-se eficiente no aumento da acurácia de classificação das CNNs [17].

A. *Transfer Learning*

Para treinar uma CNN é necessário ter um conjunto muito grande de exemplos para treinamento e teste. As redes VGG, por exemplo, foram treinadas utilizando o dataset ILSVRC-2012 [19] que contém 1000 classes e foi dividido em 3 conjuntos: 1.3 milhões de imagens para treino, 50 mil imagens para validação e 100 mil imagens para teste [17]. No entanto, imagens médicas são muito mais difíceis de se obter, principalmente com anotações de classes, devido ao tempo para realizar os estudos e para anotar todos os exemplos [16].

Uma alternativa para a utilização de CNNs com um dataset menor é a utilização do *transfer learning*. Esta técnica consiste em usar uma rede treinada com um dataset grande de imagens em um domínio mais amplo e transferir esse conhecimento para um domínio mais específico. Dessa forma, ao invés de utilizar inicialização randômica dos parâmetros, utiliza-se os pesos de uma rede já treinada. A utilização de uma rede pré-treinada reduz o tempo de treinamento e a necessidade de um dataset muito grande para o novo objetivo [20].

A aplicação do *transfer learning* pode ser feita em diversos contextos onde haja dificuldade de obter dados para treinamento. Em um survey, Shao *et al.* [21] relatam diversos usos de *transfer learning* para treinamento de redes com diferentes domínios alvo. Em oftalmologia, essa técnica mostrou-se eficiente para classificação de retinopatia diabética [22] e degeneração macular [23]. Nestes trabalhos foram utilizadas redes pré-treinadas com o dataset ImageNet, o que mostra que é possível utilizar o conhecimento de um domínio de origem mais amplo em uma tarefa específica.

B. *Redes pré-treinadas*

Entre as diversas redes convolucionais já treinadas com o ImageNet, foi escolhida a rede VGG16 para utilização neste experimento. Essa rede foi utilizada para classificação de degeneração macular com imagens de OCT no estudo de Lee *et al.* [23]. Os resultados apresentados são promissores, obtendo área sob a curva ROC de $97,46\%$.

A rede VGG16 foi utilizada no ImageNet Large Scale Visual Recognition Challenge (ILSVRC) em 2014, uma competição de reconhecimento de imagens utilizando CNNs. A rede é composta de 21 camadas com ativações ReLU, sendo 13 camadas convolucionais, 5 max pooling e 3 camadas totalmente conectadas, duas com 4096 saídas e a última com 1000 saídas de classificação. Diferente de outras arquiteturas, o VGG16 utiliza kernels menores nas camadas de convolução, o que diminui o número de pesos necessários mas ainda mantém um poder discriminativo alto. [17].

IV. Experimentos e resultados

A. *Dataset*

O dataset original foi obtido com o departamento de oftalmologia da Unicamp. O dataset consiste em imagens de OCT com tamanho 136x136 de 56 olhos com glaucoma e 66 olhos normais, totalizando 122 pacientes. Foram selecionados para o experimento somente olhos de pacientes que foram manualmente classificados por especialistas. Para a separação do dataset em treino e validação, foram selecionados 20% de olhos normais e 20% de olhos com glaucoma para validação, e o restante para treino, totalizando 98 imagens de treino e 24 de validação.

Para evitar overfitting, foi empregada técnica para aumentar o número de exemplos a partir das imagens no dataset de treino. Cada imagem foi rotacionada 100 vezes em ângulos aleatórios entre 0 e 360 graus, gerando um dataset de treino com 9800 imagens. As imagens de validação não foram rotacionadas.

B. *Pré-processamento*

Para utilização do *transfer learning*, foi necessário fazer a subtração do pixel médio. O pixel médio é calculado sobre todas as imagens do dataset de treino utilizando a equação 1, onde P_c é o valor médio por canal, M e N são as dimensões das imagens de entrada (largura e altura, respectivamente), I é a quantidade total de imagens no dataset de treino e p_{mni} é o valor do pixel na posição $\{m, n\}$ na imagem i. O valor do pixel médio é calculado em cada canal RGB, gerando um vetor de 3 posições com um valor médio por canal.

$$P_c = \frac{1}{M * N * I} \sum p_{mni} \tag{1}$$

C. *Resultados com transfer learning*

Neste experimento foi utilizada a mesma arquitetura da rede VGG16, alterando a saída da última camada totalmente conectada para duas saídas, correspondente às duas classes a serem classificadas: normal e glaucoma. Os pesos pré-treinados foram carregados para inicialização apenas das camadas convolucionais. As três últimas camadas totalmente conectadas foram inicializadas com valores aleatórios de uma distribuição normal com desvio padrão 0.01.

O treinamento foi realizado em todas as camadas da rede, utilizando o gradiente descendente estocástico por 5000 iterações, com mini *batches* de 15 imagens. Os parâmetros de *momentum* e *weight decay* foram definidos como 0.9 e 0.0005, respectivamente. A taxa de aprendizagem inicial foi de 0.001 e foi diminuída a cada 1000 iterações utilizando a equação 2, onde $base_lr$ é a taxa de aprendizagem inicial, γ é um parâmetro definido com o valor 0.1, $iter$ é o número da iteração atual e $step$ é um parâmetro definido como 1000.

$$base_lr * \gamma^{\lfloor \frac{iter}{step} \rfloor} \tag{2}$$

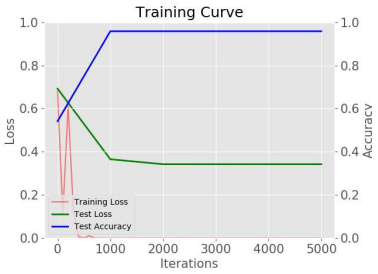


Figura 4. Acurácia e erro de treino e validação no experimento.

A validação do modelo foi feita utilizando um dataset de 24 imagens. A acurácia final obtida foi de 95.8%. O gráfico na figura 4 mostra a evolução dos valores de erro e acurácia durante o processo de treinamento. A validação foi feita a cada 1000 iterações. É possível identificar a estabilização da acurácia após 1000 iterações, quando o valor de erro do treinamento chega próximo à zero.

Os experimentos foram realizados em um servidor com duas GPUs NVidia Quadro K5200 com 8GB de memória cada. O framework de deep learning utilizado para definição da rede e treinamento em todos os experimentos foi o Caffe [24].

V. Discussão

A rede VGG16 foi escolhida para esse experimento por ter obtido bons resultados na classificação de outras doenças oftalmológicas [22], [23], porém, outras arquiteturas também podem ser utilizadas. Como trabalho futuro será feita a comparação dos resultados obtidos neste trabalho com outras CNNs.

A principal barreira neste estudo foi a quantidade limitada de dados, o que levou à utilização de técnicas para aumentar o dataset artificialmente. Ainda não foi possível determinar se as imagens rotacionadas geraram impacto no aprendizado da rede.

VI. Conclusão

Neste trabalho foram realizados experimentos com a CNN VGG16 para classificação de pacientes com glaucoma e normais a partir de imagens de espessuras da camada de fibras nervosas. Para diminuir o tempo de treinamento e permitir o uso de um dataset reduzido, foi empregada a técnica de *transfer learning* para inicializar os pesos a partir de uma rede pré-treinada com ImageNet.

Os resultados iniciais mostram que é viável o diagnóstico do glaucoma a partir das imagens de OCT. Infelizmente os resultados obtidos até o momento mostram um alto erro no dataset de validação. Uma das hipóteses para explicar o resultado é a ocorrência de overfitting devido à pequena quantidade de imagens disponíveis no dataset atual. A próxima etapa desta pesquisa será realizar novos experimentos com um conjunto estendido de imagens que está em preparação.

Referências

[1] QUIGLEY, H. A. The number of people with glaucoma worldwide in 2010 and 2020. *British Journal of Ophthalmology*, BMJ, v. 90, n. 3, p. 262–267, mar 2006.

[2] QUIGLEY, H. A. Glaucoma. *The Lancet*, v. 377, n. 9774, p. 1367 –1377, 2011.

[3] MALIK, R.; SWANSON, W. H.; GARWAY-HEATH, D. F. 'structure-function relationship' in glaucoma: past thinking and current concepts. *Clinical & Experimental Ophthalmology*, Wiley-Blackwell, v. 40, n. 4, p. 369–380, apr 2012.

[4] GRACITELLI, C. P. B.; ABE, R. Y.; MEDEIROS, F. A. Spectral-domain optical coherence tomography for glaucoma diagnosis. *The Open Ophthalmology Journal*, Bentham Open, v. 9, n. PMC4460228, p. 68–77, mar. 2015. ISSN 1874-3641.

[5] ASAOKA, R. et al. Detecting preperimetric glaucoma with standard automated perimetry using a deep learning classifier. *Ophthalmology*, Elsevier BV, v. 123, n. 9, p. 1974–1980, sep 2016.

[6] BOWD, C. et al. Bayesian machine learning classifiers for combining structural and functional measurements to classify healthy and glaucomatous eyes. *Investigative Ophthalmology & Visual Science*, v. 49, n. 3, p. 945, 2008.

[7] SILVA, F. R. et al. Sensitivity and specificity of machine learning classifiers for glaucoma diagnosis using Spectral Domain OCT and standard automated perimetry. *Arquivos Brasileiros de Oftalmologia*, scielo, v. 76, p. 170 – 174, 06 2013. ISSN 0004-2749.

[8] CHAN, T.-W. L. K. et al. Comparison of machine learning and traditional classifiers in glaucoma diagnosis. *IEEE Transactions On Biomedical Engineering*, 2002.

[9] WOLLSTEIN, G. et al. Optical coherence tomography longitudinal evaluation of retinal nerve fiber layer thickness in glaucoma. *Arch Ophthalmol*, v. 123, p. 464–471, 2005.

[10] CHAUHAN, B. C.; DRANCE, S. M.; DOUGLAS, G. R. The use of visual field indices in detecting changes in the visual field in glaucoma. *Investigative Ophthalmology & Visual Science*, v. 31, n. 3, p. 512, 1990.

[11] HUANG, D. et al. Optical coherence tomography. *Science*, American Association for the Advancement of Science, v. 254, n. 5035, p. 1178–1181, 1991. ISSN 0036-8075.

[12] Carl Zeiss Meditec. *Cirrus HD-OCT*. 2016. Disponível em: <https://www.zeiss.com/meditec/int/products/ophthalmology-optometry/glaucoma/diagnostics/oct/oct-optical-coherence-tomography/cirrus-hd-oct.html>.

[13] AREF, A.; BUDENZ, D. Spectral domain optical coherence tomography in the diagnosis and management of glaucoma. *Ophthalmic Surgery Lasers and Imaging Retina*, Slack Incorporated, v. 41 Suppl, 11 2010. ISSN 2325-8160.

[14] KROESE, M.; BURTON, H. Primary open angle glaucoma. the need for a consensus case definition. *J Epidemiol Community Health*, v. 57, p. 752–754, 2003.

[15] LECUN, Y.; BENGIO, Y.; HINTON, G. Deep learning. *Nature*, Nature Publishing Group, v. 521, n. 7553, p. 436–444, may 2015.

[16] GREENSPAN, H.; GINNEKEN, B. van; SUMMERS, R. M. Guest editorial deep learning in medical imaging: Overview and future promise of an exciting new technique. *IEEE Transactions on Medical Imaging*, v. 35, n. 5, p. 1153–1159, May 2016. ISSN 0278-0062.

[17] SIMONYAN, K.; ZISSERMAN, A. Very deep convolutional networks for large-scale image recognition. *CoRR*, abs/1409.1556, 2014.

[18] DERTAT, A. *Applied Deep Learning - Part 4: Convolutional Neural Networks*. 2017. Disponível em: <https://towardsdatascience.com/applied-deep-learning-part-4-convolutional-neural-networks-584bc134c1e2>.

[19] RUSSAKOVSKY, O. et al. ImageNet Large Scale Visual Recognition Challenge. *International Journal of Computer Vision (IJCV)*, v. 115, n. 3, p. 211–252, 2015.

[20] Tan, C. et al. A Survey on Deep Transfer Learning. *ArXiv e-prints*, ago. 2018.

[21] SHAO, L.; ZHU, F.; LI, X. Transfer learning for visual categorization: A survey. *IEEE Transactions on Neural Networks and Learning Systems*, v. 26, n. 5, p. 1019–1034, May 2015. ISSN 2162-237X.

[22] LI, X. et al. Convolutional neural networks based transfer learning for diabetic retinopathy fundus image classification. In: *2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*. [S.l.: s.n.], 2017. p. 1–11.

[23] LEE, C. S.; BAUGHMAN, D. M.; LEE, A. Y. Deep learning is effective for classifying normal versus age-related macular degeneration oct images. *Ophthalmology Retina*, v. 1, n. 4, p. 322 – 327, 2017. ISSN 2468-6530.

[24] JIA, Y. et al. Caffe: Convolutional architecture for fast feature embedding. *arXiv preprint arXiv:1408.5093*, 2014.

A review about generative adversarial networks and their applications
Um resumo sobre redes adversárias generativas e suas aplicações

OLIVEIRA, G. O.*; GOMI, E. S.*
*Laboratório KNOMA - Departamento de Engenharia de Computação e Sistemas Digitais, Escola Politécnica, Universidade de São Paulo
E-mail: {gabriel.ozeas,gomi}@usp.br

***Abstract*—Generative Adversarial Networks are one of the most popular generative models developed in the last years. They can learn representations from datasets previously not labeled. Its applicability extends through research areas as medical image processing, image synthesis, style transfer and text to image transformation. Despite this, some subtleties present in these models still enable more contribution to produce even more realistic data. This article presents the basic concepts of this unsupervised machine learning networks, besides some essential variations.**

***Keywords*— machine-learning; unsupervised learning; neural networks; generative models.**

***Resumo*— *Generative Adversarial Networks* (GAN) são um dos modelos generativos mais populares nos últimos anos. Elas permitem aprender representações de conjuntos de dados muitas vezes não previamente classificados. Sua aplicabilidade se estende por tópicos como processamento de imagens médicas, síntese de imagem, transferência de estilo e transformação entre texto para imagem. Apesar disso, algumas das sutilezas presentes nestes modelos ainda permitem mais estudos a fim de produzir dados ainda mais realistas. Este artigo apresenta os conceitos básicos destas redes de aprendizagem não supervisionada, além de algumas de suas importantes variações.**

***Palavras-chave*— aprendizagem de máquina; aprendizagem não supervisionada; redes neurais; modelos generativos.**

***Classificação*— Mestrado**

***Categoria*— Iniciante**

I. Introdução

Com a evolução do poder de processamento e a quantidade de dados disponíveis, houve um aumento significativo na quantidade estudos envolvendo *deep learning* que fazem uso destes recursos. Nos últimos dois anos, foram publicados mais de 400 artigos sobre este assunto somente na área da análise de imagens médicas [1].

Dentro da aprendizagem não supervisionada, uma das tarefas dos algoritmos de aprendizagem é encontrar estruturas ocultas subjacentes à um determinado conjunto de dados X de forma que possam ajudar a discriminá-los entre uma determinada quantidade de classes Y ou simplesmente produzir dados similares à distribuição real $P(X)$. Dentre os modelos generativos, as *Generative Adversarial Network* (GAN) apresentaram um sucesso notável nos últimos anos. Elas permitem descobrir e armazenar internamente estruturas do conjuntos de dados e podem se utilizadas para produzir dados muito semelhantes daqueles presentes na distribuição de probabilidade real. Sua aplicabilidade se estende por temas como geração de imagens [2], super-resolução [3] e conversão entre texto e imagem [4].

Este artigo tem como objetivo apresentar o conceito das GANs e algumas das suas principais variações (Seção IV). Além disso, mostrar algumas de suas aplicações em diferentes cenários que envolvem geração de dados (Seção V). Também é apresentado um experimento a partir do trabalho original [5] com o intuito de verificar a execução da técnica aplicando-a no conjunto de imagens de números manuscritos MNIST [6].

II. Trabalhos Relacionados

Atualmente existe um grande interesse no estudo de modelos generativos, um subconjunto da aprendizagem não supervisionada, devido sua vasta aplicabilidade principalmente na área da visão computacional e no processamento de imagens. Um dos problemas centrais dos modelos generativos é obter uma representação dos dados reais seja na forma de distribuições implícitas, explícitas, paramétricas ou não paramétricas [7].

Com o intuito de qualificar os diversos tipos de modelos generativos, [8] compara modelos que podem ser treinados utilizando máxima verossimilhança. Segundo ele, os modelos generativos podem ser divididos nos que produzem uma função de densidade $p_{modelo}(x, \theta)$ explicitamente, e nos modelos implícitos, que não permitem acesso a função de densidade p_{modelo}. Dentro dos modelos explícitos, eles podem ser subdivididos em tratáveis e intratáveis. Tipos como os modelos generativos auto-regressivos (PixelRNN/CNN [9]) são considerados explícitos pois aprendem funções de densidade que são acessíveis e podem ser manipuladas e avaliadas. Para cenários onde a função de densidade é intratável, modelos como *Variational autoencoders* (VAE) [10], [11] permitem aprender uma função de densidade aproximada. Juntos com as GANs, são considerados os 3 tipos de modelos generativos mais populares nos últimos anos, tanto em aplicações quanto em pesquisa [8].

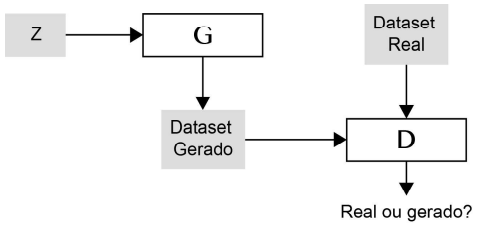


Figura 1. Generative Adversarial Network.

III. Generative Adversarial Network

As GANs compõem uma classe de métodos para a aprendizagem de modelos generativos baseado na teoria dos jogos [12]. Elas possuem a capacidade de aprender distribuições de probabilidade implícitas e, a partir delas, sintetizar dados sem a necessidade de realizar inferência durante o treinamento [5]. Caracterizam-se por serem compostas por duas funções adversárias, sendo uma função diferenciável geradora G e outra função diferenciável discriminadora D. Ambas normalmente sendo representadas por redes neurais, onde cada uma possui seu conjunto de parâmetros θ e uma função objetivo $J(\theta)$.

A tarefa da rede discriminadora D é estimar a probabilidade de uma amostra pertencer ao conjunto dos dados reais X, ou à um conjunto de dados produzido pela função G. Enquanto isso, a função G tem como tarefa tentar enganar D, produzindo dados similares a distribuição $P(X)$ 1. Porém o único compartilhando entre G e eD são os gradientes utilizados por D. O dados de entrada de G partem de uma variável ruído z, e o trabalho de G é minimizar a função objetivo $\log(1-D(G(z)))$. Ou seja, quanto mais a função D assumir que a origem dos dados produzidos pela rede geradora G pertence a distribuição $P(X)$, mais G estará perto da distribuição real. Enquanto isso, em paralelo, a função discriminadora D tenta maximizar a função $\log(D(x)) + log(1 - D(G(z)))$. A rede neural D pode também ser chamada de função de perda adversária [13] pois de certa forma ela aprende a avaliar o desempenho de G. Este cenário onde ambas as redes tentam otimizar suas funções objetivo concorrentemente, resulta em um jogo de minimax de dois jogadores onde a função valor $V(G, D)$ pode ser definida por:

$$\min_G \max_D V(D,G) = E_{x\ p_{data}(x)}[\log D(x)] + \quad (1)$$

$$E_{z\ p_z(z)}[\log 1 - D(G(z))] \quad (2)$$

As GANs são conhecidas por serem muito suscetíveis a instabilidade durante o treinamento. Um dos problemas conhecidos é chamado de *Mode collapse*, ocorre quando a função G se concentra em produzir somente um pequeno conjunto de amostras similares (colapso parcial) ou somente uma mesma amostra (colapso total) para tentar enganar a função D.

Outro problema recorrente é quando a rede discriminadora D apresenta uma alta taxa de assertividade, produzindo gradientes muito próximos de zero. Devido a dependência da rede geradora com estes gradientes, ela acaba sofrendo do problema de desaparecimento do gradiente. [14] minimiza este problema descrevendo a *Wasserstein GAN*, um modelo com uma função de custo que utiliza outra medida de distância de distribuição de probabilidade chamada de distância de *Wasserstein*.

IV. Variações de arquitetura

A. Deep Convolution Generative Adversarial Network

[2] apresentaram uma arquitetura utilizando um modelo para treinamento não supervisionado com o emprego de GANs e Redes Neurais Convolucionais (CNN) com várias camadas. Na rede neural geradora, as camadas de *pooling* foram substituídas por camadas de convolução, além de eliminarem por completo a utilização de camadas totalmente conectadas entre as camadas de convolução. Também foram adicionadas camadas de normalização de *batch* permitindo construir redes geradoras com maior profundidade sem que elas entrem em colapso. Foi demonstrado que o modelo tem desempenho competitivo quando se comparado com outros métodos de classificação não supervisionado. Além disso, os autores demonstraram a visualização das características que específicos filtros aprenderam durante o treinamento.

B. Conditional Generative Adversarial Network

[15] adicionou conceito de condicionalidade às GANs, onde além da variável ruído z, também é possível adicionar um conjunto de informações auxiliares y, permitindo gerar amostras de acordo com uma determinada categoria dentro $dataset$.

As *Conditional GANs* são utilizadas em muitas outras contribuições. [16] investigaram a utilização de *Conditional GANs* para como uma ferramenta de propósito genérico problemas que envolvem transações de imagens para imagens, através do *framework* proposto *pix2pix*. Em conjunto com a variável ruído z, também é fornecido uma imagem x para G. Tanto a rede geradora como a discriminadora utilizam uma combinação de camada de convolução, camada de normalização de *batch* e *Relu*. O *framework pix2pix* se mostrou bem versátil sendo aplicado no mapeamento de contornos para fotos e entre fotos aéreas para mapas.

V. Aplicação das GANs

Apesar do problema de alta resolução já ser investigado por outros artigos, [3] utiliza o conceito de GANs para melhorar a transformação de imagens de baixa resolução em imagens de alta resolução com um fator de escala de até 4 vezes. Ele propõe um rede adversária generativa chamada SRGAN, uma rede residual profunda (ResNet, [17]) utilizando o conceito de GANs para formar uma função de perda perceptiva. Nesta arquitetura a rede geradora G recebe como entrada uma imagem de baixa resolução e tenta gerar uma imagem de alta resolução para enganar a rede discriminadora D. Enquanto isso, a rede discriminadora tenta classificar a imagem recebida entre uma imagem normal, ou de alta resolução. [18] também apresenta um método de treinamento de GANs, onde partindo de imagens com pouco resolução e progressivamente aumentando o tamanho da rede a fim de gerar imagens com maior qualidade. A medida que o treinamento acontece, mantendo as camadas

já treinadas, novas camadas são inseridas progressivamente à redes geradora e discriminadora produzindo imagens bastante realistas a olho nu.

Um outro problema abordado por [4] é a transformação entre texto e imagem. O artigo apresenta uma arquitetura baseada em *Conditional GANs* de dois estágios. Além de um vetor de ruído z amostrado de uma distribuição gaussiana, um determinado texto é dado como entrada em uma GAN inicial produzindo imagens de baixa resolução. Logo em seguida, tanto a imagem de baixa resolução produzida, como o texto de entrada no primeiro estágio são apresentados á outra GAN capaz de imagens com maior resolução.

VI. Experimento

Para apresentar o funcionamento dos GANS, foi executado um experimento para a criação de números aleatórios manuscritos atrás de uma *Generative Adversarial Network*, onde como *dataset* de treinamento foi utilizado o conjunto de dados MNIST [6]. Foi criada uma rede neural geradora com 3 camadas totalmente conectadas. Nas primeiras duas camadas foi utilizado como função de ativação a função *Leaky Relu*[19]. Na última camada, foi utilizado como função de ativação a função tangente hiperbólica. Para a função discriminadora, foi construída uma rede neural com também 4 camadas totalmente conectadas. Para as 3 primeiras camadas além da função de ativação *Leaky Relu* também foi aplicada a técnicas de regularização *dropout* para diminuir o efeito de *overfitting* do conjunto de dados.

Para a otimização do gradiente foi utilizado o algoritmo *Adam* com uma taxa de aprendizado de $2\mathrm{e}{-4}$. Como variável de ruído foi utilizada uma distribuição normal com média 0 ± 1.0.

O treinamento foi executado com 170 épocas, onde em cada uma o dataset era particionado em conjuntos de mil imagens. Primeiro a rede D era treinada com o conjunto com dados reais, e depois com conjunto de dados gerados.

Algorithm 1 Treinamento de G e D através de *backpropagation*

for numero de epocas **do**
  for x em Minibatches(X) **do**
    m $\leftarrow tamanho(x)$
    $z_1 \leftarrow m$ amostras de $p_g \sim \mathcal{N}(0,\,1)$
    $\theta_D \leftarrow \Delta_{\theta_d} \frac{1}{m} \sum_1^m [\log D(x^i + \log 1 - D(G(z_1^i)))]$
    $z_2 \leftarrow m$ samples from $p_g \sim \mathcal{N}(0,\,1)$
    $\theta_G \leftarrow \Delta_{\theta_g} \frac{1}{m} \sum_1^m \log(1 - D(G(z_2^i)))$
  end for
end for

A figura 2 exibe uma amostra de imagens geradas a partir da rede neural geradora durante seu treinamento. Cada linha de cima para baixo corresponde as épocas 10, 30, 60, 100 e 170, respectivamente. Apesar da baixa quantidade de épocas, nota-se que a medida em que o treinamento ocorre, as imagens produzidas pela rede geradora começam a tomar formar. A partir da época 60 já é possível identificar alguns imagens semelhantes às presentes no conjunto de dados MNIST.

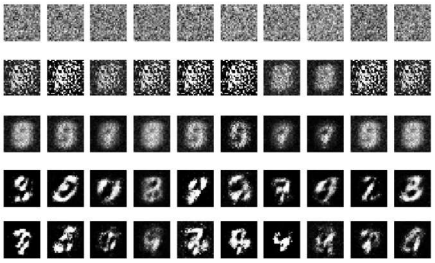


Figura 2. Amostras produzidas pela rede geradora durante o treinamento.

VII. Conclusão

As *Generative Adversarial Networks* vem sendo um dos métodos mais populares dentre os modelos generativos. Possuem diversas aplicações em tópicos como detecção de anomalias, tratamento de imagens, super-resolução e conversão entre texto e imagem. Além das GANs conseguirem aprender distribuições de probabilidade com alta dimensionalidade, seu emprego em dados não classificados torna este modelo muito propício à um vasto número de contribuições que estudam além de outras aplicações, formas de contornar os pontos fracos desta classe de métodos.

Referências

[1] Litjens, G. et al. A Survey on Deep Learning in Medical Image Analysis. *ArXiv e-prints*, fev. 2017.

[2] RADFORD, A.; METZ, L.; CHINTALA, S. Unsupervised representation learning with deep convolutional generative adversarial networks. *arXiv preprint arXiv:1511.06434*, 2015.

[3] LEDIG, C. et al. Photo-realistic single image super-resolution using a generative adversarial network. In: *CVPR*. [S.l.: s.n.], 2017. v. 2, n. 3, p. 4.

[4] ZHANG, H. et al. Stackgan: Text to photo-realistic image synthesis with stacked generative adversarial networks. *arXiv preprint*, 2017.

[5] GOODFELLOW, I. et al. Generative adversarial nets. In: *Advances in neural information processing systems*. [S.l.: s.n.], 2014. p. 2672–2680.

[6] LECUN, Y. et al. Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, IEEE, v. 86, n. 11, p. 2278–2324, 1998.

[7] SCHMIDHUBER, J. Deep learning in neural networks: An overview. *Neural Networks*, v. 61, p. 85 – 117, 2015. ISSN 0893-6080. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0893608014002135>.

[8] GOODFELLOW, I. J. NIPS 2016 tutorial: Generative adversarial networks. *CoRR*, abs/1701.00160, 2017. Disponível em: <http://arxiv.org/abs/1701.00160>.

[9] van den Oord, A.; Kalchbrenner, N.; Kavukcuoglu, K. Pixel Recurrent Neural Networks. *ArXiv e-prints*, jan. 2016.

[10] Kingma, D. P.; Welling, M. Auto-Encoding Variational Bayes. *ArXiv e-prints*, dez. 2013.

[11] REZENDE, D. J.; MOHAMED, S.; WIERSTRA, D. Stochastic backpropagation and approximate inference in deep generative models. In: XING, E. P.; JEBARA, T. (Ed.). *Proceedings of the 31st International Conference on Machine Learning*. Bejing, China: PMLR, 2014. (Proceedings of Machine Learning Research, 2), p. 1278–1286. Disponível em: <http://proceedings.mlr.press/v32/rezende14.html>.

[12] Salimans, T. et al. Improved Techniques for Training GANs. *ArXiv e-prints*, jun. 2016.

[13] ZHU, J.-Y. et al. Unpaired image-to-image translation using cycle-consistent adversarial networks. *arXiv preprint*, 2017.

[14] ARJOVSKY, M.; CHINTALA, S.; BOTTOU, L. Wasserstein gan. *arXiv preprint arXiv:1701.07875*, 2017.

[15] MIRZA, M.; OSINDERO, S. Conditional generative adversarial nets. *CoRR*, abs/1411.1784, 2014. Disponível em: <http://arxiv.org/abs/1411.1784>.

[16] ISOLA, P. et al. Image-to-image translation with conditional adversarial networks. *arXiv preprint*, 2017.
[17] He, K. et al. Deep Residual Learning for Image Recognition. *ArXiv e-prints*, dez. 2015.
[18] Karras, T. et al. Progressive Growing of GANs for Improved Quality, Stability, and Variation. *ArXiv e-prints*, out. 2017.
[19] MAAS, A. L.; HANNUN, A. Y.; NG, A. Y. Rectifier nonlinearities improve neural network acoustic models. In: *Proc. icml*. [S.l.: s.n.], 2013. v. 30, n. 1, p. 3.

VIX volatility index Prediction Using LSTM Neural Networks
Uso de Redes Neurais Recorrentes LSTM na predição do índice de volatilidade VIX

KATSUMI, F.*; GOMI, E. S.*
*KNOMA Laboratory - Department of Computer Engineering, Polytechnic School, University of São Paulo
E-mail: fabio.katsumi@gmail.com, gomi@usp.br

***Abstract*—Forecasting time series is a great challenge due to the fact that underlying processes present complex and time-variant relationships. This work provides an approach using a Long-Short Term Memory (LSTM) Recurrent Neural Network (RNN) for forecasting the implied volatility index (VIX) price one month ahead. It was used an 8 year dataset of historical prices in order to make monthly forecasts. The obtained classification accuracy was promising, achieving 53% accuracy in forecasting monthly VIX returns.**

***Keywords*— LSTM; Recurrent Neural Network; VIX.**

***Resumo*— Projetar séries temporais tem sido um grande desafio ao longo dos anos por tratar de dados com relações complexas e dinâmicas ao longo do tempo. Neste trabalho foi implementado uma Rede Neural Recorrente (RNN) do tipo *Long-Short Term Memory* (LSTM) de modo a fazer previsão de preços do índice de volatilidade implícita (VIX) um mês à frente, baseando-se em seu histórico de preços recente. Para isto, foi utilizado a série histórica de preços dos últimos 8 anos e mensalmente foram feitas projeções para o próximo mês. Os resultados obtidos foram satisfatórios, atingindo acurácia de 53% ao prever se o retorno do VIX seria positivo ou negativo no próximo mês.**

***Palavras-chave*— LSTM; Rede Neural Recorrente; VIX.**

***Classificação*— Mestrado**

***Categoria*— Iniciante**

I. Introdução

Com o crescimento da capacidade computacional em conjunto com a grande geração de dados, observa-se que a utilização de estratégias baseadas em modelos matemáticos se tornou uma das principais formas de obter retornos superiores ao custo de oportunidade no mercado financeiro.

De forma a aprofundar o entendimento na aplicação de tais estratégias, pode-se observar que uma das formas é fazer a projeção de preços baseado em algum modelo matemático, porém atualmente podemos utilizar os algoritmos disponíveis de aprendizado de máquina para nos auxiliar neste tipo de projeção.

Neste trabalho será implementado uma rede neural recorrente (RNN) *Long-Short Term Memory* (LSTM) de forma a projetar o preço do índice de volatilidade implícita (VIX), tal solução pode ser utilizada amplamente por fundos de ações para proteger o portfólio, principalmente do risco de mercado [1] ou até mesmo tomar decisões de investimento baseando-se em tais projeções.

O VIX é de extrema importância ao tomar decisões de investimento, pois é uma fonte confiável da expectativa de volatilidade do mercado de ações norte americano (S&P500) no curto prazo e representa um padrão, podendo ser comparado com outros índices similares ao redor do mundo.

II. Fundamentação Teórica

A. VIX

O VIX é um índice calculado utilizando a equação 1 pela Chicago Board of Exchange (CBOE) baseando-se nos preços das opções do S&P500 e representa a volatilidade esperada para os próximos 30 dias corridos, seguindo a metodologia publicada em [2]. O cálculo do VIX pode ser observado nas equações 1 e 2. Para isso, utilizaremos o tempo em anos até o vencimento (T), valor do strike (K), taxa livre de juros (R), valor futuro do S&P500 (F), o preço da opção (Q) e o primeiro strike abaixo do futuro (K_0).

$$\sigma^2 = \frac{2}{T}\sum_i \left(\frac{\triangle K_i}{K_i^2}\right) e^{RT} Q(K_i) - \frac{1}{T}\left[\frac{F}{K_0} - 1\right]^2 \quad (1)$$

$$VIX = 100\sigma \quad (2)$$

Opções são instrumentos financeiros mais conhecidos como derivativos, pois seu valor é uma função do preço de outro ativo (ativo subjacente), como o preço do S&P500. Existem basicamente dois tipos de opção. A opção de compra (Call) fornece o direito de compra do ativo subjacente por um preço determinado (Strike) em uma data especifica. A opção de venda (Put) fornece o direito de venda do ativo subjacente por um preço determinado em uma data especifica, como explicado em [3].

Na equação 3, como publicado em [4], o preço (Q) de uma Call pode ser calculado levando em consideração o preço atual do ativo subjacente (F), a taxa de juros (R), strike (K) e tempo em anos até o vencimento (T), dados esses obtidos no mercado, com isso podemos calcular a volatilidade

implícita (σ), levando em consideração que $N(.)$ é a função de distribuição acumulada padrão.

$$Q(K) = e^{-RT}\left[FN(d_1) - KN(d_2)\right] \tag{3}$$

$$d_1 = \frac{ln\frac{F}{K} + \sigma^2\frac{T}{2}}{\sigma\sqrt{T}} \tag{4}$$

$$d_2 = d_1 - \sigma\sqrt{T} \tag{5}$$

Como exemplo de aplicação na obtenção da volatilidade implícita, podemos considerar que o preço de uma call de S&P500 em uma determinada data era de 51.83 USD, o preço do ativo subjacente era de 930, taxa de juros 8% ao ano, strike 900 e vencimento em dois meses ou 0.17 anos. Utilizando o método **Newton-Raphson**, como em [5], podemos obter 20% de volatilidade implícita nessa opção.

Tal indice é de extrema importância na proteção de carteiras, apresentando altos retornos à medida que incertezas dos mercados aumentam, como mostrado no gráfico da figura 1, sendo assim uma das principais caraterísticas do VIX é a correlação negativa com o S&P500.

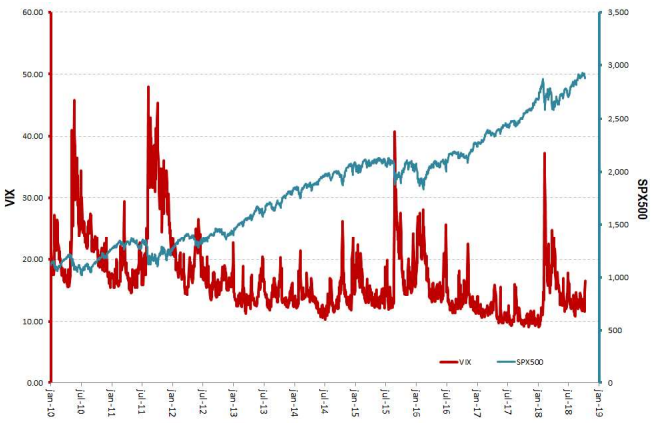


Fig. 1. VIX e S&P500

B. *Rede Neural Recorrente LSTM*

Redes neurais recorrentes são uma familia de redes neurais com foco no processamento dados sequenciais, podendo tratar sequências de dados mais longas do que outras redes neurais. Sua estrutura é similar ao de uma rede neural multicamadas, porém contém como uma das entradas as saídas dos nós anteriores. Uma RNN genérica pode ser representado pela equação 6 com modelo F, entrada x_t, estado oculto h_t para o passo t.

$$h_t = F(x_t, h_{t-1}, \theta) \tag{6}$$

A equação 6 é chamada recorrente pois h_{t-1} é usado de forma recorrente como entrada no passo t. Uma das principais ideias deste tipo de rede é o compartilhamento de parâmetros por diversas partes do modelo. Tal compartilhamento é importante quando um pedaço específico de informação ocorre diversas vezes na sequência [6] e pode ser representado pelo diagrama na figura 2.

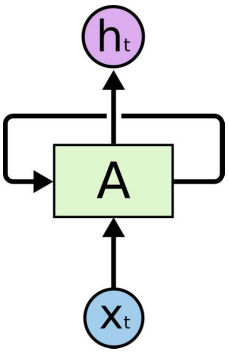


Fig. 2. Diagrama RNN [7]

RNN LSTM foram introduzidas por Hochreiter & Schmidhuber [8] de modo a resolver o problema de armazenamento de informações pela rede com grandes sequências de dados. Tal comportamento deve-se ao manter um fluxo de erro constante, porém este fluxo é controlado por meio de uma porta chamada *forget gate*, desprezando o erro quando necessário. RNN LSTM são genéricas e eficientes em capturar relações temporais de longo prazo e tem sido usadas em diversas aplicações como reconhecimento de escrita manual, tradução, modelagem acústica de fala entre outros [9]. Um diagrama da arquitetura da RNN LSTM pode ser visto na figura 3.

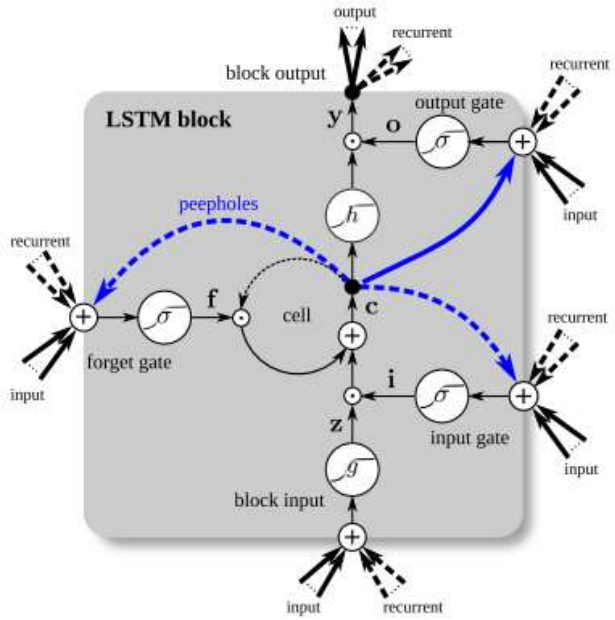


Fig. 3. Arquitetura RNN LSTM [9]

Uma RNN genérica pode ser representada pela equação 7 com modelo F_{LSTM}, entrada X_t, estado oculto h_t e estado da celula C_t para o passo t.

$$h_t, C_t = F_{LSTM}\left(x_t, h_{t-1}, C_{t-1}, \Theta\right) \tag{7}$$

O restante das equações pode ser visto a seguir.

$$f_t = \sigma\left(W_f \cdot [h_{t-1}, x_t + b_f]\right) \tag{8}$$

$$i_t = \sigma\left(W_i \cdot [h_{t-1}, x_t + b_i]\right) \tag{9}$$

$$\tilde{C}_t = tanh\left(W_c \cdot [h_{t-1}, x_t + b_c]\right) \tag{10}$$

$$C_t = f_t * C_{t-2} + i_t * \tilde{C}_t \tag{11}$$

$$o_t = \sigma\left(W_o \cdot [h_{t-1}, x_t + b_o]\right) \tag{12}$$

$$h_t = o_t * tanh(C_t) \tag{13}$$

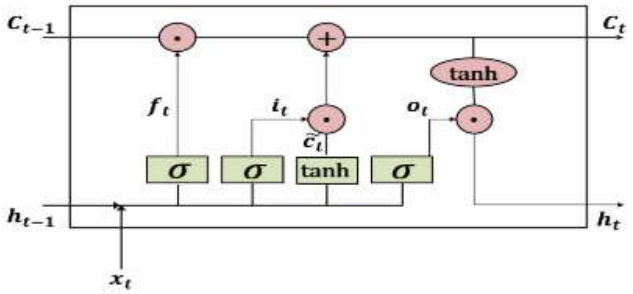


Fig. 4. Estrutura RNN LSTM

III. Experimento

Utilizando técnicas de aprendizagem de máquina conhecidas por RNN LSTM e aplicando em análise de série temporal de um ativo financeiro, foi possível testar sua performance na predição dos preços do VIX. A rede LSTM utilizada possui uma camada oculta com 200 células.

Utilizando preços diários de fechamento dos últimos 8 anos, aplicamos a RNN LSTM utilizando como entrada os preços dos últimos 21 dias e fazemos a predição para os próximos 21 dias. Tal estrategia foi escolhida, pois tende a retirar o ruído de curto prazo gerado pelos dados, gerando resultados mais robustos.

A série histórica utilizada para o treinamento do modelo varia ao longo do tempo, começando com dados de 1 ano e terminando com todo o histórico disponível.

O experimento tem como resultado a predição dos preços de fechamento dos próximos 21 dias e pode ser usada como suporte no processo decisório de investimentos.

Os dados do S&P500 e do VIX foram obtidos no site Yahoo Finance de 01/01/2010 até 31/07/2018.

As simulações foram feitas usando uma estação de trabalho desktop equipada com Intel Core i7-4790 Processor 3.6GHz, 16GB RAM. O ambiente de software utilizado foi o Python 2.7 e a LSTM foi implementada utilizando o Keras. Para cada ano de simulação tivemos um tempo de processamento de aproximadamente 90 minutos, logo para os 8 anos o tempo total de processamento foi de 6 horas e 30 minutos.

IV. Resultados

Os testes foram realizados considerando projeções feitas em todo último dia útil de cada mês para os próximos 21 dias úteis, utilizando como mês inicial 12/2010 e posteriormente as projeções foram feitas com periodicidade mensal até 07/2018. No total foram feitas projeções em 92 meses, totalizando 1932 projeções diárias (92 meses x 21 dias projetados) e para fazer a análise dos resultados foi feita a divisão das projeções em 2 grupos, o primeiro em que a projeção era de uma apreciação de preços e o segundo grupo que continha uma depreciação.

Com o agrupamento anterior, foi feita a matriz de confusão da figura 5 e podemos observar que obtivemos uma acurácia de 53% com valor preditivo positivo de 48% e valor preditivo negativo de 70%, logo observa-se que movimentos esperados de depreciação foram melhor capturados pelo modelo.

		Expectativa	
		+	-
Atual	+	33	7
	-	36	16

		Expectativa	
		+	-
Atual	+	36%	8%
	-	39%	17%

Fig. 5. Matriz de confusão

Outra forma de calcular o poder preditivo do modelo utilizado anteriormente é comparar as projeções obtidas com os dados reais, foi utilizado o *sMAPE* que siginifica média simétrica do percentual de erro absoluto dado pela fórmula 14, onde F_t é o valor projetado para determinada data e A_t é o valor real do VIX para determinada data, tal metodologia pode ser encontrada em [10]. Com isso obtivemos um erro de 18% nas projeções efetuadas.

$$sMAPE = \frac{2}{n}\sum_{t=1}^{n}\frac{|F_t - A_t|}{(F_t + A_t)} \tag{14}$$

No gráfico da figura 6, podemos observar o comportamento das projeções (azul) versus o comportamento real do ativo (vermelho), observando que à medida em que o ativo perde valor o modelo tende a projetar valores superiores ao corrente, porém quando o ativo ganha valor rapidamente o comportamento do modelo não é intuitivo, apresentando casos em que a expectativa dos próximos 21 dias é superior ao nível atual e outros que a expectativa é inferior.

V. Conclusão

Neste trabalho foi possível observar que a utilização de técnicas de aprendizagem de máquina são promissoras em projeções de séries temporais, assim como feito com a série do VIX. O comportamento de preços obitido nas projeções

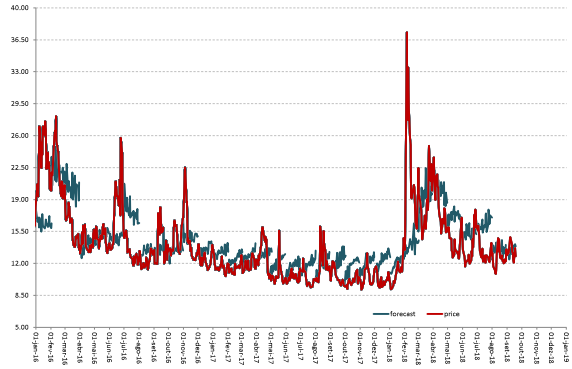


Fig. 6. Índice VIX vs Projeção

atendeu a expectativa, apresentando comportamentos muitas vezes não lineares e sua perfomance foi satisfatória tanto em relação à acurácia quanto em relação ao sMAPE obtido.

Como trabalho futuro planejamos utilizar como entrada do modelo outras informações, como séries de preços de outros ativos, indicadores financeiros da economia e informações sobre a saúde financeira das empresas americanas.

REFERENCES

[1] DAMODARAN, A. *Investment Valuation*. [S.l.]: Wiley Finance, 2002.
[2] CBOE. Vix: Cboe volatility index. 2003.
[3] HULL, J. C. *Options, Futures, and Other Derivatives*. [S.l.]: Prentice Hall, 2002.
[4] BLACK, F. The pricing of commodity contracts. *Journal of Financial Economics*, p. 161–179, 1976.
[5] WILMOTT, P. *Paul Wilmott On Quantitative Finance*. [S.l.]: Wiley, 2006.
[6] GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. *Deep Learning*. [S.l.]: MIT Press, 2016.
[7] OLAH, C. Understanding lstm networks. *http://colah.github.io/posts/2015-08-Understanding-LSTMs/*.
[8] HOCHREITER SEPP URGEN SCHMIDHUBER, J. Long short-term memory. *Neural Computation*, v. 9, p. 1, 1997.
[9] GREFF, K. et al. LSTM: A Search Space Odyssey. *IEEE Transactions on Neural Networks and Learning Systems*, v. 28, n. 10, p. 2222–2232, 2017. ISSN 21622388.
[10] ARMSTRONG, J. S. *Long-Range Forecasting: From Crystal Ball to Computer*. [S.l.]: Wiley, 1985.

Identity theft detection using trajectory patterns
Detecção de roubo de identidade utilizando padrões de trajetória

SILVA, G. M. C. *; SICHMAN, J. S. *;
*Laboratório de Técnicas Inteligentes - Escola Politécnica da Universidade de São Paulo
E-mail: gabrielmariano@usp.br, jaime.sichman@usp.br

***Abstract*—One of the major organizations' concerns is unauthorized access to their valuable information and assets. When it comes to physical access control, identity theft is one of the most common fraud types. Several studies involving identity theft detection have been conducted, but very few have approached the physical user access. In the present work, we propose to detect insider threats of identity theft in a building access control system by finding anomalies in individual and group trajectories. The proposal is to build users' mobility profiles that incorporates informations of locations, times and social groups. In order to support the detector implementation, we have set up an agent-based simulation framework using Gamma Platform and R environment, which proved to be consistent tools to address project's needs.**

***Keywords*— insider threat; identity theft; trajectory pattern mining; multi-agent-based simulation; mabs;**

***Resumo*— O acesso não autorizado a dados e ativos de valor é um dos principais problemas das organizações, dado o atual contexto da segurança da informação. Referente aos dados de controle de acesso físico, o roubo de identidade é o tipo de fraude mais comum. Segundo o referencial teórico, muitos estudos envolvendo detecção de roubo de identidade foram realizados, no entanto, apenas um pequeno percentual de trabalhos abordada o acesso físico dos usuários. Neste artigo, propomos detectar ameaças internas de roubo de identidade em um sistema de controle de acesso predial, por meio da detecção de anomalias em trajetórias dos usuários. Nossa proposta é construir um perfil de movimentação de usuários, o qual incorpore informações de locais, tempos e também de grupos sociais, de forma que novas trajetórias que não sejam compatíveis com perfil construído sejam consideradas anomalias. Para suportar a construção do detector, estabeleceu-se uma metodologia de simulação com o ambiente R e a plataforma Gamma.**

***Palavras-chave*— ameaça interna; roubo de identidade; mineração de padrões em trajetórias; simulação baseada em multiagentes**

***Classificação*— Mestrado**

***Categoria*— Iniciante**

I. Introdução

Crimes e fraudes contra organizações têm crescido ao longo dos últimos anos, como aponta o estudo encomendado pela Kroll para a *The Economist Intelligence Unit* [1]. Das ocorrências de fraude em que o autor foi identificado, quatro em cada cinco (81%) envolvia pelo menos uma pessoa de dentro da empresa. Nesse caso, quando ataques são cometidos por membros da própria organização, as ofensas são chamadas de "ameaças internas".

Para aumentar a segurança, organizações limitam o acesso a seus sistemas e instalações físicas a somente membros da organização ou a associados externos de sua confiança e somente a recursos mínimos necessários para execução de suas tarefas. Sistemas de controle de acesso predial especificam locais, horários, condições e regras que determinam como as pessoas se movimentam no espaço físico. O controle de acesso físico é baseado em identidades, de forma que cada indivíduo deve ser identificado unicamente e as regras de acesso devem ser validadas em tempo real pelo sistema. Muitos tipos de credenciais são utilizadas, sendo que entre as mais comuns temos senhas (algo que se sabe), cartões RFID, de tarja magnética ou códigos de barras (algo que se possui), impressões digitais, padrões vasculares, íris, retina e estruturas ósseas da face (biometria).

Ameaças às organizações são frequentemente protagonizadas por integrantes da própria organização, a quem foram concedidos privilégios legítimos de acesso e, portanto, consistem em uma ameaça interna. Para os casos em que a ameaça interna é realizada propositalmente com objetivo de causar dano ou obter vantagem, os ofensores são classificados entre "traidores" e "mascarados" [2]. Um traidor é um usuário membro de uma organização a quem foi concedido legítimo acesso a sistemas, instalações físicas e recursos de informações, mas cujas ações são contrárias às políticas da organização. Um mascarado, por sua vez, rouba a identidade de um colega integrante da mesma organização e se faz passar por ele.

A identidade humana tem manifestações sociais, pessoais, psicológicas e comportamentais que podem ser observadas. O local de trabalho, a frequência com que a pessoa se ausenta, horários de costume de chegada e saída, caminho preferido e grupos sociais podem ser inferidos com a observação dos registros dos sistemas de controle de acesso predial. Um sistema especialista poderia utilizar essas informações para identificar se uma identidade foi roubada.

Há duas principais abordagens na detecção automática de fraudes de roubo de identidade: *baseada em assinaturas*, quando os ataques são bem conhecidos e seus efeitos podem ser rastreados rapidamente, ou *baseada em anomalias*, quando são conhecidos apenas os dados normais de operação do sistema e uma novidade será considerada uma ameaça. No entanto, estudos sobre roubo de identidade na literatura científica se concentram em fraudes contra instituições finan-

ceiras (e.g. cartão de crédito) [3] e não há dados suficientes em outros domínios, o que inviabiliza a detecção de fraudes por assinatura em outras organizações. Por outro lado, trajetórias de seres humanos possuem alto grau de regularidade espaço-temporal e seguem simples padrões reproduzíveis [4].

A mineração de dados de trajetórias é um tema bastante recorrente na literatura [5]. Um exemplo é a extração de padrões de grupo, que visa detectar grupos de objetos que se movem juntos. Os padrões mais estudados são hordas, comboios e enxames. Padrões de movimento individual de objetos são outra classe da mineração de trajetórias. Em [6], os autores formalizam a construção de perfis de mobilidade individual de pessoas e propõe uma métrica de similaridade e distância entre perfis, expandindo o trabalho previamente desenvolvido em [7]. Os perfis de mobilidade são construídos com uso de T-Patterns (do inglês *trajectory patterns*) [8], que são um exemplo de mineração de padrões de trajetória frequentes. Não há, porém, uma formulação de perfis de mobilidade individuais que incluam as relações sociais dos indivíduos.

A hipótese deste estudo é que ataques internos de roubo de identidade podem ser detectados quando observadas anomalias (valores aberrantes ou *outliers*) nas trajetórias de movimentação de pessoas dentro de um prédio. Nosso objetivo é propor uma formulação de perfil de mobilidade individual de usuários que inclua os grupos com os quais os usuários se relacionam e que possa ser comparada com novas trajetórias de modo que que, caso não coincidam com o perfil histórico do usuário, sejam consideradas uma ameaça. Para auxiliar a futura implementação do algoritmo detector, propomos uma simulação baseada em agentes que reproduzam os perfis de mobilidade estudados.

Este trabalho se organiza da seguinte maneira: na seção II revisitamos a literatura que serve de base para proposição do nosso modelo. Na seção III propomos uma teoria unificada de perfil de mobilidade que envolve espaço, tempo e grupo social. Na seção IV propomos uma metodologia para desenvolvimento do algoritmo de extração de perfis e seu aprimoramento. Na seção V mostramos os resultados parciais já obtidos e os resultados esperados. A seção VI traz a conclusão e propostas de trabalhos futuros.

II. Trabalhos anteriores

Uma trajetória é uma sequência de pontos espaço-temporais (s, t) cronologicamente ordenados [9]. Há duas abordagens possíveis para essa anotação temporal dos espaços: atribuir a posição espacial a intervalos fixos no tempo (como faz um sistema GPS) ou anotar a hora em que objeto atinge pontos fixos predefinidos no espaço (pontos de verificação, como mostra a Tabela I). Para fins e mineração de padrões, quando o que importa são as regiões de interesse (RI) e tempos de transição, os dados de GPS são tratados conforme a tabela I.

A. Perfis individuais de trajetórias

Um padrão de trajetória (*T-Pattern*) de um usuário representa um dos traços de mobilidade regulares do usuário [8].

Tabela I
Dados obtidos de um sistema de pontos de verificação

Data e Hora	Usuário	Ponto de verificação (RI)
2018-03-24 08:30:04.557	61983	Garagem
2018-03-24 12:13:55.123	61983	Docas
2018-03-24 13:07:15.578	61983	Portaria
2018-03-24 17:30:38.965	61983	Armazém

O padrão é representado por $Tu = (S, A)$ onde u é o usuário, $S = (s_0, ..., s_n)$ é uma sequência de lugares e $A = (\alpha_1,...,\alpha_n)$ são os tempos de transição entre os lugares, também podendo ser representado por:

$$Tu = s_0 \xrightarrow{\alpha_1} s_1 \xrightarrow{\alpha_2} ... \xrightarrow{\alpha_n} s_n. \quad (1)$$

Se em uma trajetória um usuário transita sequencialmente em todos os lugares de um *T-Pattern* e gasta tempo semelhante para a transferência entre os lugares, então dizemos que esse *T-Pattern* é espaço-temporalmente contido nessa trajetória.

Um perfil de mobilidade $PS^{Tu}_{\tau,\sigma}$ descreve o movimento frequente de um usuário, ou seja, as sequências de lugares que o usuário costuma visitar [6]. Ele é formado por um conjunto de padrões frequentes (*T-Patterns*). A frequência das ocorrências de padrões (S, A) em um conjunto de dados é quantificada pela porcentagem de trajetórias que as contêm, o que é chamado de valor de suporte. A função suporte retorna a proporção em que determinado padrão (S, A) aparece em relação a todos os padrões (S, A) do usuário. Quando a tolerância para o intervalo de tempo $\alpha \in A$ estiver definida para τ, a função suporte é denotada por $suporte^{Tu}_{\tau}(S, A)$. Dado um conjunto de trajetórias Tu do usuário, um tempo de tolerância τ e um valor mínimo de suporte σ, o conjunto de padrões frequentes (τ, σ) será:

$$PS^{Tu}_{\tau,\sigma} = \{(S, A) | suporte^{Tu}_{\tau}(S, A) \geq \sigma\}. \quad (2)$$

Uma das aplicações dos perfis de mobilidade é encontrar usuários com perfis semelhantes [6], mas eles também podem servir para identificar se uma trajetória não contém nenhum dos padrões frequentes do perfil, sendo então um valor aberrante (*outlier*). Os conjuntos de padrões frequentes são uma boa construção dos perfis de mobilidade de pessoas em termos de espaço (locais em que o usuário esteve presente) e tempo (duração do deslocamento). No entanto, não trazem informações sobre interações sociais dos usuários. Na movimentação de pessoas em um prédio, é possível observar o comportamento regular de pessoas que se deslocam em conjunto.

B. Padrões de grupo

Os padrões de movimentação em grupo mais estudados são hordas, comboios e enxames, ilustrados na Figura 1, que foi adaptada de [10]. Uma horda é um grupo de usuários que viajam juntos por registros de data e hora consecutivos, de modo que, em qualquer uma dessas marcações de tempo, eles são encontrados espacialmente dentro de um disco circular.

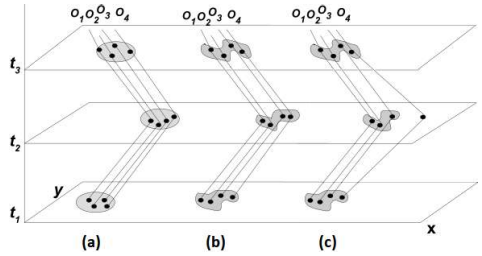


Figura 1. Exemplos de padrões de grupo (a) horda (b) comboio e (c) enxame adaptados de [10]

Nos comboios, o agrupamento espacial pode assumir qualquer forma e em geral são utilizados agrupamentos baseados em densidade. A definição de enxame [11] é uma evolução comboios que relaxa a restrição de marcações de tempo consecutivas.

Nos padrões de enxame, temos uma série de usuários $U_{DB} = \{u_1, u_2, ..., u_n\}$ e marcações de tempo $T_{DB} = \{t_1, t_2, ..., t_m\}$ referentes ao deslocamento desses usuários. Grupos $G_{DB} = \{G_{t_1}, G_{t_2}, ..., G_{t_m}\}$ são coleções de capturas instantâneas dos grupos de objetos em movimento em cada marcação de tempo. $G_{t_i}(u_j)$ é utilizado para denotar o conjunto de grupos aos quais o objeto u_j pertence no instante t_i.

Um par (U, T) é um enxame se todos os objetos em U estão em um mesmo grupo em qualquer marcação em T. Dados dois limiares mínimos min_u e min_t, para (U, T) ser um enxame, onde $U = \{u_{i_1}, u_{i_2}, ..., u_{i_p}\} \subseteq U_{DB}$ e $T \subseteq T_{DB}$, é necessário:

- $|U| \geq min_u$: U deve ter no mínimo min_u usuários.
- $|T| \geq min_t$: Os usuários em U devem estar no mesmo grupo por no mínimo min_t marcações de tempo.
- $G_{t_i}(u_{i_1}) \cap G_{t_i}(u_{i_2}) \cap ... \cap G_{t_i}(u_{i_p}) \neq \emptyset$ para qualquer t_i em T, isto é, que haja pelo menos um grupo contendo todos os usuários de U a cada marcação de tempo em T.

Para evitar a identificação de enxames redundantes, é dada ainda a definição de enxame fechado. Um enxame (U, T) é usuário-fechado se, fixando-se T, U não pode ser aumentado; é dito temporalmente fechado se fixando-se U, T não pode ser aumentado. O enxame (U, T) é um enxame fechado se é simultaneamente usuário e temporalmente fechado. Em [11] são propostos algoritmos eficientes para extração de enxames fechados em um banco de dados.

Para o modelo proposto, acreditamos que os perfis de mobilidade dos usuários formados por *T-Patterns* podem ser enriquecidos com informações de grupos, e mais especificamente, de enxames.

III. Modelo proposto

No modelo proposto, o perfil de mobilidade do usuário pretende indicar não só *onde* e *quando*, mas também *com quem* acessa o local com frequência. Um padrão de trajetória T de um usuário u_j pode ser definido como $T = (S, A, U)$ onde $S = (S_0, ..., S_n)$ é uma sequência de lugares em que o usuário esteve, $A = (\alpha_1, ..., \alpha_m)$ são anotações temporais da sequência, e $G = (G_0, G_1, ..., G_n)$ a sequência de grupos que u_j pertence em cada marcação de tempo. De outra forma:

$$T = (s_0, G_0) \xrightarrow{\alpha_1} (s_1, G_1) \xrightarrow{\alpha_2} ... \xrightarrow{\alpha_n} (s_n, G_n). \quad (3)$$

O perfil de mobilidade PS^u de um usuário u é o conjunto de padrões de trajetórias T de um usuário. Dado um conjunto de trajetórias como descrito anteriormente, um tempo de tolerância τ e um valor mínimo de suporte σ, o padrão frequente (τ, σ) é

$$PS^{Tu}_{\tau,\sigma} = \{(S, A, G) | suporte^{Tu}_{\tau}(S, A, G) \geq \sigma\}. \quad (4)$$

Após a construção dos perfis de mobilidade baseada em dados históricos dos usuários, pretendemos implementar um detector de anomalias que identificará, em tempo real, uma trajetória de um usuário que não corresponda com seu perfil.

IV. Metodologia

Os registros de acessos de usuários em um sistema de controle de acesso são semelhantes aos observados na Tabela I. A partir desse tipo de conjunto de dados, pretendemos identificar quando os usuários transitam em grupos e os possíveis enxames (U, T) formados. Para isso, utilizaremos o software R [12], uma poderosa plataforma aberta para computação estatística. A plataforma R também será utilizada para a construção dos perfis dos usuários e detecção de trajetórias de usuários que não contenham um padrão de seu perfil histórico, o que pode indicar uma fraude de roubo de identidade.

Pretendemos validar a formulação proposta em ambientes reais. Porém, dificilmente será possível obter dados de sistemas muito diversos para refinamento do modelo. Para auxiliar na implementação dos algoritmos que construirão os perfis de mobilidade, propomos uma simulação do ambiente real na qual será possível alterar o número de usuários, tamanho médio dos grupos formados, diferentes turnos de trabalho (noturno, diurno, 12x36) e demais variações. A simulação permitirá o entendimento de quais variáveis min_u, min_t. τ e σ são mais adequados para cada ambiente. Cada rodada de simulação ocorrerá em três etapas.

- treinamento, em que agentes simulam trajetórias normais e escolhem grupos.
- gera o banco de trajetórias (tabela I) e calcula o perfil PS^u de cada agente.
- trajetórias anômalas são inseridas artificialmente e observamos na simulação e observamos o desempenho do decetor.

Pela necessidade de uma simulação de aplicação de tempo real em um ambiente complexo envolvendo decisões individuais de pessoas, acreditamos que a abordagem multi-agentes baseada em modelos mentais, em especial os modelos de raciocínio prático BDI (*belief-desireintention*) [13], serão mais apropriadas para o desenvolvimento da simulação. A simulação será construída utilizando a plataforma Gamma

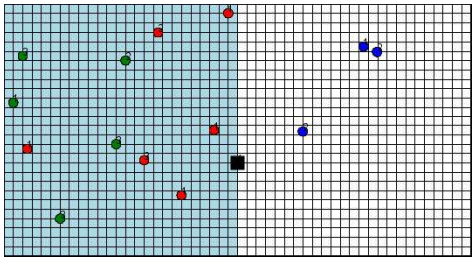


Figura 2. Simulação de movimentação em um prédio utilizando a plataforma Gamma

[14], que permite a implementação de agentes reativos e também BDI que se comunicam utilizando performativas FIPA [15]. Há integração com sistemas de dados de sistemas de informação geográfica (*GIS*) e integração nativa com R, o que faz com que os códigos desenvolvidos para o detector possam interagir em tempo real com a simulação. A plataforma inclui ainda ferramentas para modelagem de relacionamento entre os agentes, que utilizaremos para indicar relações de grupo.

V. Prova de conceito e resultados parciais

Para avaliarmos as ferramentas escolhidas e integrações entre elas, construímos uma simulação de movimentação de pessoas em um prédio. A Figura 2 mostra a área interna do prédio representada com fundo azul e a área externa com fundo branco. Modelamos dois tipos de agentes: agente Portaria e agente Usuário. Cada agente Usuário representa uma pessoa frequentadora do prédio. A cada rodada da simulação, os agentes usuários são inicializados com um conjunto de amigos. Os amigos são representados com cores iguais na Figura 2. A intenção inicial dos usuários é apenas entrar no prédio para trabalhar. Para fazerem isso, solicitam autorização de entrada ao agente Portaria (representado pelo quadrado em preto no centro da Figura 2) utilizando a performativa FIPA ”Request”. O agente Portaria é um agente reativo que apenas autoriza o acesso para todos os usuários, indistintamente, e escreve as movimentações em um arquivo CSV. A cada novo dia, é atualizada no agente Usuário uma variável ”fome” com valor igual a zero e um limiar de fome com valor aleatório. Conforme o tempo passa, a ”fome” dos usuários aumenta linearmente. Uma vez que a fome de um usuário ultrapassa seu limiar de fome, o agente assume uma nova crença de ”fome” e uma intenção de ir almoçar. Então, convida os amigos para almoçar utilizando a performativa FIPA ”Propose”. Seus amigos reativamente aceitam o convite e então vão todos em grupo almoçar. A Figura 2 mostra os amigos azuis retornando do almoço.

De tempos em tempos, a simulação chama um script em R que recebe os registros de movimentação de todos os usuários. O script utiliza algoritmos de agrupamento (k-means) para identificar a qual grupo pertence cada usuário. Por fim, o script retorna os grupos encontrados, que a simulação exibe em tela com um número ao lado de cada agente Usuário.

VI. Conclusão e Trabalhos futuros

Neste artigo, definimos a hipótese de que um usuário que realiza uma trajetória que não corresponda com seu perfil histórico de movimentação pode ter sido vítima de roubo de identidade. Para construção de perfis de mobilidade [6], propomos uma evolução dos padrões de trajetórias [8] incorporando dados de enxame [11]. Para auxiliar na implementação de um detector de roubo de identidade, foi proposta uma solução de simulação baseada em agentes utilizando o ambiente de simulação Gamma Platform e sua integração nativa com software R, uma solução que se mostrou robusta e que auxiliará na adequação da implementação aos vários tipos de cenários possíveis. Para continuidade deste trabalho, pretendemos provar a regularidade dos padrões de trajetória com cálculos de entropia [16] no cenário observado. Vamos complementar a simulação já realizada, incorporando capacidades aos agentes que ilustrem mais situações da vida real, como recusas de convites e imprevistos na chegada ao prédio, adicionando maior estocasticidade à simulação. Desejamos também que o detector interaja com a simulação para impedir novos acessos de usuários suspeitos de terem sido vítimas de roubo de identidade.

Referências

[1] KROLL. Kroll Global Fraud Report. *Annual Edition 2015/2016*, 2015.

[2] SALEM, M. B.; HERSHKOP, S.; STOLFO, S. J. A survey of insider attack detection research. *Insider Attack and Cyber Security*, Springer, v. 298, n. 0704, p. 69–90, 2008.

[3] HOOFNAGLE, C. J. Identity theft: Making the known unknowns known. *Harv. JL & Tech.*, HeinOnline, v. 21, p. 97, 2007.

[4] GONZALEZ, M. C.; HIDALGO, C. A.; BARABASI, A.-L. Understanding individual human mobility patterns. *Nature*, Nature publishing group, v. 453, n. 7196, p. 779, 2008.

[5] FENG, Z.; ZHU, Y. A survey on trajectory data mining: techniques and applications. *IEEE Access*, IEEE, v. 4, p. 2056–2067, 2016.

[6] CHEN, X.; PANG, J.; XUE, R. Constructing and comparing user mobility profiles. *ACM Transactions on the Web (TWEB)*, ACM, v. 8, n. 4, p. 21, 2014.

[7] YING, J. J.-C. et al. Mining user similarity from semantic trajectories. In: ACM. *Proceedings of the 2nd ACM SIGSPATIAL International Workshop on Location Based Social Networks*. [S.l.], 2010. p. 19–26.

[8] GIANNOTTI, F. et al. Trajectory pattern mining. In: ACM. *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining*. [S.l.], 2007. p. 330–339.

[9] GIANNOTTI, F.; NANNI, M.; PEDRESCHI, D. Efficient mining of temporally annotated sequences. In: SIAM. *Proceedings of the 2006 SIAM International Conference on Data Mining*. [S.l.], 2006. p. 348–359.

[10] MAZIMPAKA, J. D.; TIMPF, S. Trajectory data mining: A review of methods and applications. *Journal of Spatial Information Science*, v. 2016, n. 13, p. 61–99, 2016.

[11] LI, Z. et al. Swarm: Mining relaxed temporal moving object clusters. *Proceedings of the VLDB Endowment*, VLDB Endowment, v. 3, n. 1-2, p. 723–734, 2010.

[12] TEAM, R. C. et al. R: A language and environment for statistical computing. Citeseer, 2013.

[13] BRATMAN, M. *Intention, plans, and practical reason*. Cambridge, MA: Harvard University Press, 1987.

[14] GRIGNARD, A. et al. Gama 1.6: Advancing the art of complex agent-based modeling and simulation. In: *International Conference on Principles and Practice of Multi-Agent Systems*. Berlin, Heidelberg: Springer, 2013. p. 117–131.

[15] FIPA Communicative Act Library Specification. 2002. Disponível em: <http://www.fipa.org/specs/fipa00037/SC00037J.html>.

[16] SONG, C. et al. Limits of predictability in human mobility. *Science*, American Association for the Advancement of Science, v. 327, n. 5968, p. 1018–1021, 2010.

Information Retrieval-Based Question Answering System
Sistema de Question Answering Baseado em Recuperação de Informações

POL, FLÁVIO.; GOMI, EDSON.; (Flávio Jaime Pol Gonçalves; Edson S. Gomi)
KNOMA/PCS - Escola Politécnica, Universidade de São Paulo
E-mail: {flaviopol; gomi}@usp.br

***Abstract*—A lot of human knowledge is in textual form which is a form of information registration for future references. In many cases, searching for specific information in these set of texts can be time-consuming. The evolution of natural language processing has provided solutions to reduce this delay. This article presents the implementation of a Question Answering System based on Information Retrieval where the reader can ask an objective question about a set of texts and the system obtains the answer based on these textual references. To obtain the answer the system uses machine learning algorithms, specific rules and frequency of the words in the texts.**

***Keywords*— Natural Language Processing; Information Retrieval; Question Answering.**

***Resumo*— Grande parte do conhecimento humano encontra-se na forma textual que é uma forma de registro das informações para futuras consultas. Em muitos casos, a busca por informações específicas nesses conjunto de textos pode ser demorada. A evolução do processamento de linguagem natural tem proporcionado soluções para diminuir essa demora. Este artigo apresenta a implementação de um sistema de perguntas e respostas baseado em Recuperação de Informação onde o leitor pode realizar uma pergunta objetiva referente a um conjunto de textos e o sistema obtém a resposta baseado nessas referências textuais. Para obter as respostas o sistema utiliza algoritmos de aprendizado de máquina, regras específicas e a frequência das palavras nos textos.**

***Palavras-chave*— Processamento de Linguagem Natural; Recuperação de Informação; Sistema de Perguntas e Respostas.**

***Classificação*— Mestrado**

***Categoria*— Iniciante**

I. Introdução

Em diversas áreas do conhecimento, grande parte da informação se encontra na forma textual, alguns desses registros podem ser: processos judiciais, prontuários médicos, artigos científicos, relatórios de manutenção, atas de reunião, ocorrências policiais, entre outros. O objetivo dessa informação textual é registrar o conhecimento para futuras consultas, no entanto ler essa documentação é uma tarefa que exige tempo e disposição, uma vez que realizar buscas por informações específicas não é uma tarefa simples, e as diversas áreas do conhecimento estão em constante atualização. O objetivo deste artigo é apresentar a implementação de um Sistema de Question Answering baseado em Recuperação de Informações onde perguntas objetivas sobre um conjunto de textos possam ser respondidas em respostas curtas. O *Question Answering System* QAS permite buscar a resposta em uma grande quantidade de documentos textuais e dessa forma pode auxiliar leitores na busca rápida por informações, assim o QAS pretende contribuir na diminuição do tempo gasto pelos leitores nesse processo de busca.

A seção II descreve a metodologia do QAS, a seção III descreve a implementação do QAS, o algoritmo, conjunto de dados e os resultados.

II. Metodologia

A implementação do QAS tem como base o método de Question Answering Baseado em Recuperação de Informações (IRQA) do capítulo 28 do livro(draft) *Speech and Language Processing. Daniel Jurafsky & James H. Martin.* [1], também conhecido como Text-Based Question Answering [2]. Este método depende de um documento disponível na forma de texto, e para uma pergunta, utilizam-se técnicas de recuperação de informação para extrair respostas diretamente do documento, considerando as palavras isoladas ou n-gramas do texto da pergunta. O método foca em *Factoid Questions* (FQ) que são perguntas que podem ser respondidas com um fato simples expresso em respostas curtas de texto, por exemplo: nome, data, localização. O autor também apresenta um paradigma IRQA híbrido amplamente conhecido como o Watson da IBM [3].

O método IRQA é composto por 3 principais estágios: Processamento da pergunta *(Question Processing)*, Recuperação de Frases *(Passage Retrieval)* e Processamento da Resposta *(Answer Processing)*. A figura 1 apresenta os 3 estágios do método IRQA. O primeiro estágio recebe a pergunta do usuário e processa para alimentar o segundo e terceiro estágios. O segundo estágio processa os documentos também fornecidos pelo usuário. O terceiro e último estágio processa as informações dos estágios prévios para obter a resposta da pergunta do usuário. Cada estágio utiliza regras, scores, rankings e pesos para definir a relevância da palavra, n-grama, parágrafo ou frase do documento.

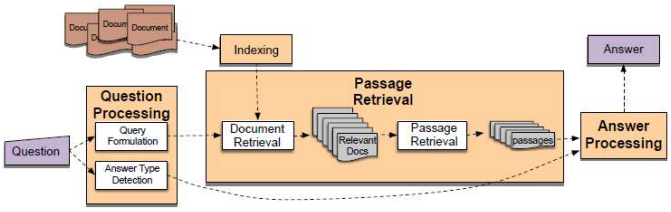


Figura 1. Os 3 estágios do método IRQA: Question Processing, Passage Retrieval and Answer Processing.

A. Processamento da Pergunta

O objetivo desta etapa do IRQA é extrair o máximo de informações do texto da pergunta para alimentar as etapas posteriores. Por exemplo, para a pergunta: *Which US state capital has the largest population?*, aplicam-se:

- Detecção do tipo de resposta: *Location* → Tipo da classe da resposta
- Formulação da pergunta: *US state capital, largest, population* → Palavras-chave para consulta nos documentos.
- Foco da pergunta: *state capital* → *String* que será substituída pela resposta
- Tipo da pergunta: equação matemática, lista → definição da pergunta, alguns sistemas possuem.

1) Detecção do tipo de resposta: A subetapa de detecção do tipo de resposta tem como objetivo determinar a que classe a resposta pertence baseado apenas no texto da pergunta. Para esta classificação utilizam-se algoritmos *machine learning* (ML) e/ou regras escritas manualmente [4].

Na classificação com algoritmos ML, utilizou-se para treinamento algumas *features*, tais como: *Part of Speech Tagging* (POS), *Named Entity Recognition* (NER), *Chunking* (CK), mais detalhes na seção III-A. O conjuntos de dados rotulados para esta finalidade TREC https://trec.nist.gov fornecem +5000 perguntas para treinamento e testes. Em geral, a acurácia na classificação de perguntas são relativamente altas em tipos de perguntas fáceis, como perguntas sobre um indivíduo ou grupo, localização, número e datas.

2) Formulação da pergunta: Também conhecida como *Query Formulation*, consiste em criar a partir do texto da pergunta uma lista de palavras-chaves *(query)* que serão utilizadas na etapa seguinte para consultar nos documentos. Para obter melhores resultados, esta lista possui pesos para cada palavra que possibilita a ponderação de cada palavra. Para expandir ou definir os pesos dessa lista podemos aplicar:

- Expansão da lista que implica em utilizar sinônimos para aumentar o número de palavras.
- Hiperonímia e hiponímia que são palavras que fazem parte da semântica.
- A frequência do termo–inverso da frequência (IDF) nos documentos [1].

O trabalho *Machine learning for query formulation in question answering* [5] apresenta 18 features que podem ser utilizadas para definir os pesos da lista.

B. Recuperação de Frases

Na etapa de Recuperação de Frases, a lista ponderada utiliza-se para consultar um índice que contém as palavras mais relevantes por documento. O resultado intermediário deste estágio é o conjunto de documentos e seus parágrafos mais relevantes. Como resultado final, são extraídas as frases mais relevantes dos parágrafos.

1) Indexação de documentos: A subetapa de indexação de documentos acontece previamente à execução do sistema IRQA e consiste em organizar o corpus (conjunto de documentos) utilizando o IDF das palavras desse corpus. Esta organização gera um índice das palavras mais relevantes do corpus e a sua frequência em cada documento do conjunto. Após gerar o índice, selecionam-se os documentos onde as palavras da lista da pergunta mais ocorrem, então são adicionados para recuperação dos parágrafos e frases nas subetapas seguintes. Nesta subetapa também aplicam-se a retirada de *stopwords*, e suprimem-se prefixos e sufixos com *stemmer* e *lemma* se necessário.

2) Recuperação de Parágrafos: Nesta subetapa ponderam-se os parágrafos mais relevantes do documento escolhido. Para isso aplica-se a similaridade de cosseno entre a lista de palavras da pergunta e o parágrafo dos documentos selecionados. Nesta etapa pode-se escolher o número de parágrafos mais relevantes que serão utilizados na etapa seguinte.

3) Recuperação da Frase: A subetapa de Recuperação de Frases calcula-se semelhanças entre a pergunta e a frase para criar uma lista ponderada. Esse cálculo consiste na comparação de n-gramas, que podem ser unigramas, bigramas, trigramas, entidade e tipo de Resposta.

C. Processamento da Resposta

Para a subetapa de Processamento da Resposta aplicam-se dois métodos para a extração da resposta: Extração de Padrões *(Pattern Extraction)* e *N-gram Tiling*. Para ambos métodos a resposta pode ser única ou vir acompanhada com contextualização.

A técnica de Extração de Padrões utiliza a informação esperada do tipo de resposta II-A1 junto com padrões de expressões regulares. Este método não funciona muito bem para classes que a resposta seja uma definição, para estes casos podemos escrever regras que combinem a *Question Phrase* (QP) e a *Answer Phrase* (AP). Para este último caso, também pode-se utilizar ML para automatizar a extração de padrões. Esses padrões podem ser usados em conjunto a informações para serem classificadas em um ranking baseado em *features*: *Answer Type*, *Pattenr match*, *number of matched question keywords, keywords distance, novelty factor, apposition features, pontuaction location, sequences of question terms*.

A técnica *N-gram Tiling* é mais utilizada para QAS na Web, onde inicia com a comparação de n-gramas nos trechos de textos do resultado do buscador, nessa fase os uni-gramas, bi-gramas ou tri-gramas são extraídos dos trechos de texto e ponderados por quantas vezes o n-grama apareceu no trecho. O próximo passo é o *N-filtering* onde os n-gramas são classificados por quão similares são da resposta em potencial em II-A1.

Esses scores são feitos por filtros escritos para cada tipo de resposta. O ultimo passo é o *Ngram tiling* onde concatenam-se os n-gramas que se sobrepõem para formar uma resposta mais longa. Para obter a resposta final utiliza-se a resposta candidata com o maior score.

III. Implementação Factoid Question Answering

Para desenvolver o sistema QA utilizou-se a linguagem Python 3.6 e a biblioteca de funções para processamento de linguagem natural NLTK *(Natural Language Toolkit)*.

A. NLTK

O NLTK foi originalmente criado em 2001 como parte de uma disciplina em linguística computacional no *Department of Computer and Information Science da University of Pennsylvania*. Para este experimento utilizamos os módulos Part-of-speech tagging nltk.tag, Chunking nltk.chunk, Stopwords nltk.stopwords, steemer nltk.stem, Processamento de Strings nltk.tokenize.

B. Algoritmo

O algoritmo 1 apresenta o QAS implementado.

processCorpus Processa o texto referência para o sistema QA. Para cada parágrafo do texto executam-se as seguintes operações:

- Remove *stopwords* de cada parágrafo se **removeStopWord** for verdadeiro
- Aplica *stemmer* de cada parágrafo se **useStemmer** for verdadeiro
- Contabiliza a frequência de palavras $TermFrequency$ para cada parágrafo e armazena em **wordFrequency**
- Contabiliza a frequência de uma palavra específica em cada parágrafo do texto e a armazena em **wordParagraphFrequency**. Se a palavra existe no parágrafo, contabiliza +1, caso contrario, 0.
- Calcula a frequência do termo–inverso da frequência nos documentos (IDF) utilizando Laplace smoothing 1.

$$\text{idf}_t = \log \frac{N}{df_t} (1)$$

  Armazena em **paragraphInfo** um índice para cada parágrafo: 'wF' contendo *wordFrequency* e 'vector' contendo o produto da frequência da palavra e seu idf.

processAskedQuestion Processa a pergunta inserida pelo usuário e aplica **removeStopWord** e **useStemmer** caso verdadeiro. Também inclui a opção da utilização de sinônimos para expansão da consulta *(query expantion)* caso **useSynonyms** verdadeiro. Estes sinônimos provém do Dicionário *Wordnet*

qType Armazena o tipo da pergunta para 5W1H dentre as seguintes opções:

$$who \rightarrow WP; what, why, how \rightarrow WDT$$

$$whose \rightarrow WP\$; where \rightarrow WRB; None \rightarrow others$$

aType Utiliza regras para determinar o tipo de resposta esperada dependendo do qType. As opções são: *Person,Location,Date,Organization, Quantity, Definition, Full*

Algorithm 1 Sistema Question Asnwering

```
1:  procedure processCorpus(inputText)        ▷ Procedure for the Corpus
2:      for all paragraphsCorpus do
3:          if removeStopWord == TRUE then
4:              paragraphsCorpus ← stopwords()
5:          else if useStemmer == TRUE then
6:              paragraphsCorpus ← PorterStemmer()
7:          end if
8:          wordFrequency ←computeTFIDF(paragraphsCorpus)
9:          wordParagraphFrequency ←computeTFIDF(wF)
10:         idf ←computeTFIDF(wPF)
11:         paragraphInfo ←computeTFIDF(wF,wF*idf)
12:     end for
13: end procedure

14: procedure processAskedQuestion(input)
15:     question ← input
16:     if removeStopWord == TRUE then
17:         question ← stopwords()
18:     else if useStemmer == TRUE then
19:         question ← PorterStemmer()
20:     else if useSynonyms == TRUE then
21:         question ← wordnet()
22:     end if
23:     qType ←determineQuestionType(question)
24:     aType ←determineAnswerType(question)
25:     searchQuery ←buildSearchQuery(question)
26:     qVector ←getQueryVector(searchQuery)
27:     for response ←query(question,qVector,aType,idf) do
28:         for revelantParagraph ←getSimilarParagraph() do
29:             queryVectorDistance ←sum((qVector*idf)*2)/2
30:             pRanking ←computeSimilarity()
31:         end for
32:         sentences ←getSentencesFrom3relevantParagraph
33:         for relevantSentences ←getMostRelevantSentences() do
34:             sim ←sim_ngram_sentence()
35:             sim ←sim_sentence()
36:         end for
37:         if aType == PERS;LOC;ORG;DATE;[NP;NNP];DEF then
38:             ne ← getNamedEntity()
39:             ne ← extractDate()
40:             ne ← getContinuosChunk()
41:         end if
42:         answer ←firstSentenceMostRelevant
43:     end for
44:     response ←answer
45:     print response
46: end procedure
```

searchQuery Tokenização da pergunta e aplica a expansão da consulta com sinônimos caso *useSinonyms* verdadeiro.

qVector Armazena em um vetor as palavras e seu respectivo peso que é definido pela frequência em em *searchQuery*.

revelantParagraph Obtém os 3 parágrafos mais relevantes com base na similaridade de cosseno entre o vetor da pergunta *qVector* e vetor de parágrafo*pInfo*. **revelantSentences** Após extrair as sentenças dos parágrafos de *relevantParagraph* obtem-se as sentenças mais relevantes usando a semelhança de unigramas entre a sentença da pergunta e a sentença no parágrafo que contém a resposta em potencial.

response Após obter as sentenças mais relevantes de *relevantSentences*, utiliza-se o *aType* para processamento da resposta *(Answer Processing)*. Nessas sentenças mais relevantes, aplicam-se regras específicas dependendo do *aType*.

C. Conjunto de dados

O conjunto de dados utilizado nesta implementação é o SQuAD *(Stanford Question Answering Dataset)* [6]. É um conjunto de dados voltado à compreensão de texto, consistindo em perguntas sobre artigos da Wikipédia, onde a resposta para cada pergunta é um segmento de texto ou extensão do trecho de texto correspondente ou a pergunta pode ser irrespondível.

D. Resultados

A tabela I apresenta os resultados dos testes com alguns textos do conjunto de dados SQuAD. A acurácia para cada um dos 12 textos, que somavam 3840 perguntas, obteve-se por divisão simples da resposta correta pelo numero total de perguntas (2). A acurácia do QAS foi diferente para cada texto e a acurácia total foi de 70,16% .

$$\text{Acurácia} = \text{N}^{\text{o}} \text{ respostas corretas} \,/\, \text{N}^{\text{o}} \text{ total de perguntas} \quad (2)$$

A tabela II apresenta alguns exemplos de perguntas, a resposta do QAS e a resposta esperada. A pergunta 1 tem a resposta esperada. Nas perguntas 2 e 3 a resposta veio acompanhada do contexto. As perguntas 4 e 5 tiveram as respostas esperadas, porém não completas. Na pergunta 6 a resposta está incompleta e na pergunta 7 a resposta está errada.

Tabela I
RESULTADOS DO TESTES SISTEMA QA EM 12 TEXTOS DE TEMAS DIVERSOS

Tópico do Texto	Perguntas	Corretas	Acurácia (%)
New_York_City	817	513	62.79
Buddhism	610	428	70.16
Queen_Victoria	680	378	55.59
Modern_history	448	325	72.54
Windows_8	202	148	73.27
USB	235	208	88.51
Marvel_Comics	123	77	62.6
Mammal	88	59	67.05
Alloy	96	65	67.71
Rajasthan	119	82	68.91
NW_University	227	165	72.69
Anthropology	222	178	80.18

IV. CONCLUSÕES

O QAS implementado neste artigo obteve uma acurácia razoável de 70,16% considerando que, segundo [6], a compreensão humana para responder perguntas é aproximadamente 86,83%. A implementação do QAS utilizou da metodologia de recuperação de informações para perguntas objetivas onde as respostas esperadas são sucintas. Devido a esse método, algumas das perguntas que obtiveram respostas erradas possuíam mais de um tipo de resposta esperada (ex: nome, data) dentro da mesma sentença, o que ocasionou a classificação equivocada. Uma melhoria no sistema seria a utilização de menos regras especificas, e para esses casos, talvez ter maior uso de sistemas de aprendizagem profunda *(Deep Learning)*.

Tabela II
EXEMPLOS DE PERGUNTAS SQUAD, RESPOSTA DO SISTEMA QA E A RESPOSTA ESPERADA

Pergunta	Resposta Sistema QA	Resposta Esperada
1. What country was the second largest source of foreign-born New Yorkers in 2011?	china	china
2. The U.S. military has only one active location in NYC named what?	new york city is home to fort hamilton, the u.s. military's only active duty installation within the city.	fort hamilton
4. Who was believed to be the father of Lady Flor's "baby"?	conroy	sir john conroy
6. Who are Windows main operating system competitors?	android	android and ios
7. The New York Stock exchange is located where in NYC?	london	wall street

Para os testes, a implementação utilizou um conjunto de dados em língua inglesa e para execução utilizou classificadores *machine learning* (POS, NER, CK) treinados nesse idioma. Já para implementar o mesmo sistema QA deste artigo em língua portuguesa ou em outra língua, precisaria treinar os classificadores especificamente no idioma, além de possuir um conjunto de dados sólido para testes do sistema.

REFERÊNCIAS

[1] JURAFSKY, D.; MARTIN, J. H. *Speech and language processing: An introduction to natural language processing, computational linguistics, and speech recognition*. [S.l.]: Prentice Hall, Pearson Education International, 2009. 1–1024 p.

[2] CHRISTOPHER, D. M.; PRABHAKAR, R.; HINRICH, S. Introduction to information retrieval. *An Introduction To Information Retrieval*, v. 151, n. 177, p. 5, 2008.

[3] FERRUCCI, D. et al. Building watson: An overview of the deepqa project. *AI magazine*, v. 31, n. 3, p. 59–79, 2010.

[4] LI, X.; ROTH, D. Learning question classifiers: the role of semantic information. *Natural Language Engineering*, Cambridge University Press, v. 12, n. 3, p. 229–249, 2006.

[5] MONZ, C. Machine learning for query formulation in question answering. *Natural Language Engineering*, Cambridge University Press, v. 17, n. 4, p. 425–454, 2011.

[6] RAJPURKAR, P. et al. Squad: 100, 000+ questions for machine comprehension of text. *CoRR*, abs/1606.05250, 2016. Disponível em: <http://arxiv.org/abs/1606.05250>.

Modelo de suporte à decisão para Seleção de pessoas baseado em Mineração de dados

SOUSA, I. A. N.*; SPINA, E.*; † (Ítalo Alberto do Nascimento Sousa; Edison Spina)
* PCS - Engenharia de Computação e Sistemas Digitais
†CEST - Centro de Estudos Sociedade e Tecnologia
E-mail: italoengenharia@usp.br, spina@usp.br

***Resumo*— A área de Analytics tem crescido de maneira expressiva tanto em escopo como em variedade de aplicações. Organizações têm investido de maneira crescente nos últimos anos na área da gestão de Recursos Humanos. Dentre as principais aplicações de Analytics, destaca-se a área de HR Analytics, uma abordagem que se baseia em dados para tomar melhores decisões sobre pessoas em uma organização. A mineração de dados destaca-se como um dos principais meios de obtenção de resultados para viabilizar essa prática. Estudos que envolvem HR Analytics têm crescido nos últimos anos, mas poucas dessas investigações realizam trabalhos quantitativos ou experimentais. Dentre as principais áreas de HR Analytics, destaca-se o processo de seleção de pessoas, pois ele determina a qualidade do pessoal que entra na organização. Nesta pesquisa, é abordado um estudo de caso de um processo de seleção onde a cada processo há mais inscritos e fica mais difícil selecionar os melhores candidatos. A partir disso, é trazida uma proposta de modelo de suporte para tomada de decisão que leva em consideração os critérios principais de seleção baseado na aplicação de mineração de dados em um processo de seleção. Os resultados indicam que os critérios de avaliação desse processo podem ser melhorados com a escolha dos critérios principais de seleção e que o uso dessa metodologia de mineração de dados pode contribuir com a otimização do processo de seleção.**

***Palavras-chave*— HR Analytics; Mineração de dados; Processo de Seleção; Critérios principais; Tomada de decisão.**

***Classificação*— Mestrado**

***Categoria*— Em conclusão**

I. Introdução

A área de gestão de RH (Recursos Humanos) tem recebido investimentos de maneira crescente nos últimos anos dentro das organizações. Esta área é reconhecida cada vez mais como um diferencial estratégico na busca por crescimento e vantagem competitiva [1] [2].

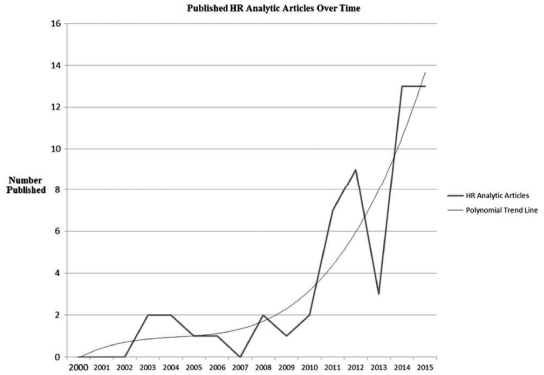
Com o avanço da computação, pesquisadores têm desenvolvido sistemas de suporte à decisão, sistemas especialistas e usado análise de dados para melhorar os resultados da gestão de RH. A área de análise de dados, ou em inglês *Analytics*, têm crescido de maneira expressiva tanto em escopo como em variedade de aplicações [3] [4].

Dentre as principais aplicações de *Analytics*, destaca-se a área de *HR (Human Resources) Analytics*. *HR Analytics* é uma abordagem que se baseia em evidência para tomar melhores decisões sobre pessoas em uma organização.

Nesse contexto, a mineração de dados destaca-se como um dos principais meios de obtenção de novos resultados para estudos analíticos [4]. Mineração de dados se refere aos métodos utilizados para viabilizar a prática de *Analytics* [3]. Ela consiste no processo de identificação de padrões originais e válidos baseado no uso de dados [6].

Estudos que envolvem essas abordagens de *HR Analytics* e suas aplicações têm crescido de maneira expressiva nos últimos anos, como pode ser visto na figura 1 [5].

Figura 1. Publicações em HR Analytics.



Dentro da grande área de Recursos Humanos, destaca-se o Processo de Recrutamento e Seleção. Esse processo é o responsável por agregar as competências e os talentos necessários para contribuir na busca por vantagem competitiva nas organizações diante de um contexto altamente dinâmico e complexo. Apesar desses dois termos serem comumente abordados como uma só função, as atividades de cada um variam. O processo de Recrutamento consiste na procura e atração de candidatos para uma determinada função requerida na organização. Já o processo de Seleção, consiste na tomada de decisão do candidato a ser escolhido para atuar em determinada função da organização [1] [7].

A partir disso, esta pesquisa tem como objetivo propor um modelo de suporte para tomada de decisão em um processo de seleção baseado em mineração de dados.

II. HR Analytics

A. Processo de Seleção

O processo de Seleção de pessoas possui um papel fundamental na gestão de RH, pois determina a qualidade de entrada do pessoal em uma organização. Ele consiste na comparação do padrão de características dos candidatos com um referencial estabelecido para o processo de seleção. Esse rigor de escolha ocorre com o intuito de manter ou aumentar o desempenho do pessoal. Ele deve ser levado com especial atenção pois define qual candidato vai ficar com a vaga [4] [1] [7].

Uma organização busca encontrar por meio de um processo de seleção os candidatos que mais se aproximam do seu perfil desejado, e assim fazem por meio de filtros [7]. Esses filtros são compostos por diferentes atividades dentro de diferentes etapas, como dinâmicas em grupo, testes individuais e entrevistas.

B. Mineração de dados

A mineração de dados consiste em uma série de técnicas que possuem diferentes abordagens para solucionar problemas. De maneira geral, são métodos avançados de análise de dados utilizados para trabalhar com variáveis em busca de padrões razoáveis [8][9].

Os principais métodos utilizados para mineração de dados são a classificação, predição, regras de associação, análise preditiva, redução de dados, visualização e exploração de dados, aprendizado supervisionado e não supervisionado [9] [3].

As técnicas de mineração citadas fazem parte do fundamento para o uso de *HR Analytics*. O conceito de *HR Analytics* consiste em ferramentas e tecnologias que variam desde relatórios simples de métricas até a elaboração de modelos preditivos [5].

III. Metodologia de pesquisa

A. Estudo de caso

O processo de seleção abordado nesta pesquisa é baseado em dados reais de uma Organização da Sociedade Civil que atua com assistência social. Nesta organização, são elaborados critérios de avaliação que buscam aumentar o conhecimento sobre os candidatos e sintetizar o que é esperado de um candidato para exercer com bom desempenho as atividades propostas.

Os dados utilizados nesta pesquisa são os resultados dos critérios adotados no processo de seleção de avaliação dos candidatos. São realizadas duas etapas para avaliação e geração de pontuação no processo de seleção, a dinâmica em grupo e a entrevista individual. Eles contemplam a quantidade de 252 dados brutos dos candidatos pelos quais passam pela etapa de processamento e resultam em 131 dados analíticos, os quais representam as instâncias utilizadas nesta análise.

Na etapa da dinâmica em grupo, cada candidato recebe uma nota, de zero a cinco, e conta com os critérios de avaliação: Iniciativa (*Initiative*), Organização (*Organization*), Trabalho em equipe (*Team work*), Motivação (*Motivation*), Comprometimento (*Commitment*) e Comunicação (*Communication*). Nessa etapa, ele pode ser A (Aprovado) ou R (Reprovado) pelo avaliador. Na etapa da entrevista individual são praticamente os mesmos critérios, com exceção da Iniciativa. E então, pode ser A (Aprovado), R (Reprovado), ou sujeito a V (Verificação) para deixar a decisão do status de aprovação do candidato para o fim do processo.

Na entrevista, há um critério singular da Assiduidade (*Attendance*), porém ele é isolado e não contribui na geração da pontuação para seleção dos candidatos, apenas contribui como peso de decisão nos desempates. Esse critério é gerado por meio de uma pergunta simples e direta sobre a participação de cada candidato no programa. Ele é categorizada pelo avaliador, com as opções de resposta:

- A: candidatos que têm certeza de que irão para o final e absolutamente não faltarão;
- B: candidatos que pensam que vão até o fim, mas talvez venham a faltar algum dia;
- C: candidatos que não têm muita certeza se irão até o final.

B. Modelo de suporte à decisão

Segundo os membros da organização, a cada processo há mais inscritos e fica mais difícil tomar decisões no processo de seleção apenas com o somatório das pontuações coletadas na dinâmica e na entrevista.

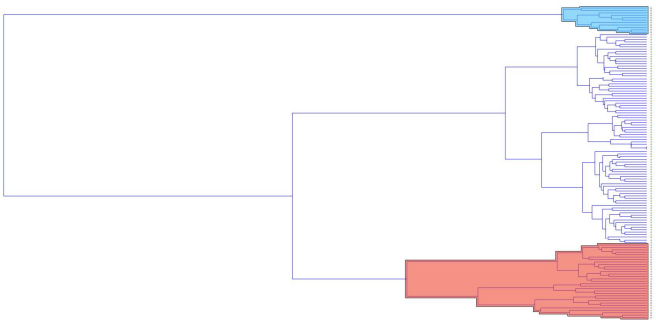
Durante o processo da análise para seleção, alguns candidatos possuem pontuações bem altas, então são candidatos praticamente certos de serem selecionados. Outros já possuem pontuações bem baixas, o que já os tornam bastante propícios a serem reprovados. A dificuldade na seleção encontra-se nos candidatos que não possuem pontuações tão claras de serem aprovados ou reprovados de acordo com os critérios de seleção. Esse problema fica ainda maior quando aumenta-se o número de candidatos, pois aumenta-se a incerteza na análise para seleção.

Para explorar os dados do processo de seleção e conseguir melhorá-lo, utilizam-se técnicas de mineração de dados que se encaixam nesse problema, como a classificação. Por meio da técnica de clusterização chamada de Agrupamento, candidatos com pontuação de critérios semelhantes são agrupados e grupos com pontuações diferentes são divididos. Baseado nos dados da seleção, tem-se o agrupamento representado pela figura 2. Os grupos não-destacados são compostos totalmente pelos candidatos aprovados. Os grupos destacados em azul e vermelho representam o agrupamento dos candidatos amplamente rejeitados.

A partir disso, verifica-se que o grupo azul representa todos os candidatos reprovados, e já o grupo vermelho representa os candidatos que possuem características semelhantes de reprovação, mas que possuem alguns candidatos bem sucedidos. Ou seja, o grupo vermelho possui no geral candidatos com pontuações semelhantes nos

critérios mas que por algum motivo são aprovados. Esse acontecimento indica que há três grupos de candidatos levados em consideração para tomada de decisão, o que tem características de aprovado, o que tem de reprovado e o que tem característica incerta para seleção.

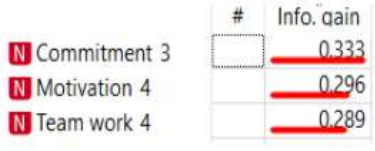
Figura 2. Agrupamento pelas pontuações dos critérios.



Para explorar esse acontecimento, busca-se saber no agrupamento vermelho o que difere os candidatos aprovados dos demais. Para isso, realiza-se um ranking dos critérios que trazem o maior ganho de informação para a análise de aprovação. Os resultados obtidos trazem a resposta de quais critérios possuem o maior peso na avaliação, ou seja, quais são os critérios principais de seleção.

Na dinâmica em grupo, o melhor ganho de informação vem do Trabalho em equipe, depois da Comunicação e Iniciativa. Na entrevista individual, ele vem do Comprometimento, seguido pela Motivação e Trabalho em Equipe, visto pela figura 3. Esse ganho de informação representa quais critérios influenciam mais no pesado da tomada de decisão, ou seja, quais são os critérios principais para tomadas de decisão.

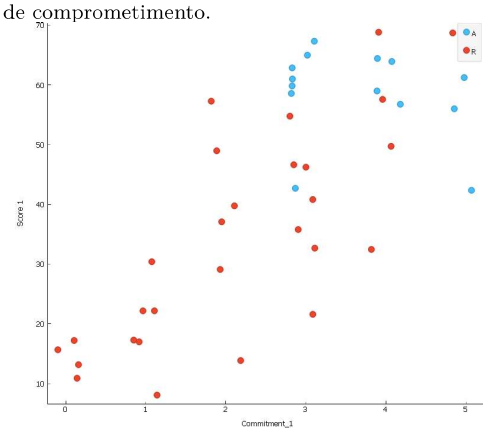
Figura 3. Ranking do ganho de informação dos critérios.



Na análise do quão diferentes esses candidatos bem sucedidos diferem dos demais, o gráfico de dispersão é usado para verificar qual é a relação entre esses candidatos e as pontuações dos critérios. Ao verificar cada item, nota-se que aqueles que oferecem maiores valores de Comprometimento ou Trabalho em Equipe, apesar de terem características predominantemente semelhantes aos reprovados, possuem maior probabilidade de serem aprovados na seleção.

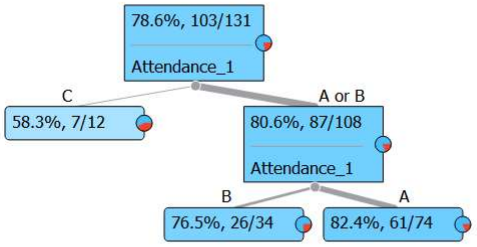
Como o critério Comprometimento é a que traz o maior ganho de informação, analisa-se, por meio do agrupamento vermelho, o gráfico da dispersão dos candidatos aprovados em relação às suas pontuações, visto pela figura 4. Este gráfico indica que candidatos com maiores pontuações de Comprometimento, mesmo tendo várias semelhanças com outros reprovados, conseguiram aprovação.

Figura 4. Gráfico de dispersão da pontuação pela aprovação do critério de comprometimento.



Utiliza-se uma árvore de decisão para classificar as pessoas que respondem mais positivamente à pergunta simples e final sobre o desejo de comparecer de forma assídua ao programa de formação, como pode ser visto pela figura 5. Nota-se então, que os candidatos que tiveram a maior taxa de aprovação em todas as etapas do processo foram aqueles que tiveram o maior nível de Assiduidade nessa pergunta final.

Figura 5. Árvore de decisão da porcentagem de aprovação pelo nível de Assiduidade dos candidatos.



A partir disso, são estabelecidos quais são os critérios principais de seleção tanto para a dinâmica em grupo quanto para a entrevista individual. Esses critérios principais são obtidos baseados na classificação dos resultados de aprovação e reprovação dos candidatos de acordo com as pontuações correspondentes de cada critério avaliado.

C. Modelo de suporte a decisão

Processos de seleção contam com candidatos a serem selecionados e critérios para realizar essa seleção. A fase de decisão leva em conta tais critérios como forma de decidir quem é ou não selecionado. Candidatos com pontuações

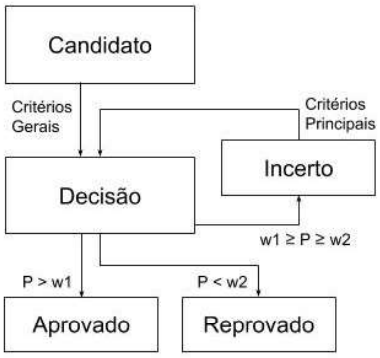


Figura 6. Modelo de suporte a decisão para Seleção de pessoas.

P acima de determinado limiar w1, representado pela equação 1, costumam ser aprovados sem dificuldades, que é o caso do grupo não-destacado descoberto pelo agrupamento da figura 2. Da mesma forma candidatos com pontuações P abaixo de outro limiar w2, representado pela equação 2 e pelo grupo azul da figura 2, costumam ser reprovados também sem dificuldades. Porém, o grupo de candidatos que possuem pontuações P que se encontram entre esses dois limiares, representado pela equação 3 e pelo grupo vermelho da figura 2, são os que merecem maior atenção na melhora de um processo, pois são os que trazem maior dificuldade de seleção. Além disso, esse limiares w1 e w2 dependem de cada processo de seleção analisado, pois representam o ponto de separação ótimo entre candidatos totalmente aprovados e totalmente reprovados no processo. Esse limiar pode ser obtido pela aplicação dos dados do novo processo de seleção no modelo antigo de seleção de um processo realizado na organização, onde são conhecidos os resultados da classificação anterior. Já os critérios principais podem ser reaproveitados a cada processo, e além disso, podem ser continuamente refinados por meio de novas descobertos de quais critérios influenciam mais no ganho de informação de cada processo.

$$P > w1 \tag{1}$$

$$P < w2 \tag{2}$$

$$w1 \geq P \geq w2 \tag{3}$$

Por meio dos resultados obtidos, é gerado um modelo representado pela figura 6, que sintetiza o processo de decisão onde é levado em consideração tanto a comparação das pontuações com os limiares w1 e w2, quanto o uso dos critérios principais para revisão das decisões.

Da mesma forma que os critérios gerais de seleção oferecem informações úteis para suportar a decisão sob os candidatos, critérios que trazem mais informação na decisão dessas seleções podem também ser úteis nesse suporte a tomada de decisão. Os critérios principais funcionam como uma revisão para aqueles candidatos que não tiveram sua decisão de aprovação ou reprovação plenamente definida apenas com os critérios gerais, os candidatos incertos.

IV. Conclusões

Nesta pesquisa, busca-se contribuir com uma investigação quantitativa da mineração de dados aplicada ao contexto de *HR Analytics*. Para isso, busca-se investigar uma das áreas mais prioritárias da gestão de RH, que é o processo de seleção de pessoas, pois ele quem define as qualidades e competências do pessoal que vai fazer parte da organização. A ideia da utilização de mineração de dados para o processo de seleção é deixá-lo mais objetivo utilizando os fatos como suporte na tomada de decisão e não as impressões.

Baseado nos experimentos elaborados, esta pesquisa traz como contribuições resultados tanto para a organização trabalhada quanto para a área de HR Analytics. Na organização trabalhada, são descobertos os seus principais critérios utilizados para seleção. Na área de HR Analytics, é realizado um estudo quantitativo e experimental de uma das suas principais frentes, a seleção de pessoas.

Destaca-se como contribuição desta pesquisa a proposta de um modelo de suporte para tomada de decisão em um processo de seleção, que pode ser aplicado para diferentes processos de seleção que possuam critérios de avaliação e candidatos incertos. Pois sem a descoberta dos critérios principais, todos os critérios são tratados com a mesma importância, e portanto, a tomada de decisão para os candidatos incertos torna-se menos objetiva, o que pode trazer mais dificuldade para seleção no processo.

Agradecimentos

Este trabalho foi realizado durante uma bolsa de estudos financiada pelo CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico). Agradecimento ao apoio do CEST (Centro de Estudos Sociedade e Tecnologia). Agradecimento à ONG Instituto CEO do Futuro (http://ceodofuturo.org.br/) pelos dados da pesquisa.

Referências

[1] BAYLãO, A. L. da S.; ROCHA, A. P. de S. A importância do processo de recrutamento e seleção de pessoal na organização empresarial. 2014.

[2] DULEBOHN, J. H.; JOHNSON, R. D. Human resource metrics and decision support: A classification framework. 2013.

[3] SHMUELI, G. et al. Data mining for business analytics: Concepts, techniques, and applications in r. 2017.

[4] CHIEN, C.-F.; CHE, L.-F. Data mining to improve personnel selection and enhance human capital: A case study in high-technology industry. 2006.

[5] MARLER, J. H.; BOUDREAU, J. W. An evidence-based review of hr analytics. 2016.

[6] STROHMEIER, S.; PIAZZA, F. Domain driven data mining in human resource management: A review of current research. 2012.

[7] CAXITO, F. de A. *Recrutamento e Seleção de Pessoas*. 1. ed. [S.l.: s.n.], 2012.

[8] HAN, J.; KAMBER, M.; PEI, J. *Data mining: concepts and techniques*. 3. ed. [S.l.: s.n.], 2012.

[9] SHMUELI, G. et al. *Data Mining for Business Analytics: Concepts, Techniques, and Applications*. 3. ed. [S.l.: s.n.], 2016.

Efficient Methods for Knowledge Transfer Augmented by Natural Language Processing

LIMA PAIVA, F. C.; COSTA, A. H. R.
Laboratório de Técnicas Inteligentes (LTI)
Escola Politécnica da Universidade de São Paulo
E-mail: {francisco.paiva, anna.reali}@usp.br

***Abstract*—The objective of this masters research is to contribute with a framework that uses task knowledge expressed in textual natural language (NL) in order to facilitate the transfer of knowledge between different tasks, aiming to accelerate Reinforcement Learning (RL) in a new task. Although techniques for transferring knowledge between tasks in RL have been explored previously in the literature, few have explored the use of natural language texts to abstract tasks and use these texts to facilitate learning in a new task. The present research aims to analyze qualitatively and quantitatively the existing proposals, and from this comparative analysis to define improvement points to guide the proposal, development and validation of a new framework that uses texts to represent abstract problems, so that they can be useful to accelerate the solution of new RL problems. Our framework will be tested in different domains, including games and chatbots.**

***Keywords*— Reinforcement Learning; Transfer Learning; Natural Language Processing; Chatbots.**

***Classification*— Master's degree.**

***Category*— Beginner.**

I. Introduction

Reinforcement learning (RL) is one of the most active areas of research in the machine learning universe, and its various fields of study have evolved and matured continuously [1]. An RL agent is punished or rewarded according to the outcome of its actions, allowing it to learn how to proceed on the basis of past triumphs or losses. RL aims to learn an actuation policy that maximizes the expected sum of the rewards received by the agent, based on the trial and error approach. RL is very powerful as it allows the agent to achieve its objective with very little human interference. However, it may take many iterations to converge, even for smaller problem space and so, its ability to learn in complex environments may be reduced [2], [3].

Lately, the use of deep RL has enabled several complex problems to be solved [4], [5], [6]. However, learning time is still a major limitation. This has led to the emergence of the Transfer in RL field [7], [8], which consists of a series of proposals and research aimed at using the knowledge previously acquired in learning previous tasks to accelerate the learning of new tasks. It is important to note that in order to successfully use a transfer learning method, it is generally desirable to have similarities between the state and action spaces of the different domains. One approach that has proven effective in transferring knowledge is learning generalized policies that work across domains [9], [10]. However, one of the most prominent research directions of transfer learning has used natural language as the basis for state representation, which makes it possible to learn policies that generalize more effectively to new domains [11]. Also, these methods have been studied in several applications such as human robot speech interaction, and promising results have been achieved [12].

In our work we want to show that the use of environment description in natural language may not only be effective for transfer learning but also complement other approaches that transfer generalized policies between tasks. In particular, we use a variation of the classical Markov decision processes (MDPs) [13] representation, the Object-oriented Markov decision process (OO-MDP) formalism, to explore the relations of state and dynamics of objects in a task. We believe that this representation enables a greater generalization between different tasks [14]. Our research aims to propose, develop and validate a new framework that uses texts to represent abstract problems in OO-MDP formalism so that these texts can be used to accelerate the solution of new RL problems.

To perform the validation and comparative analysis of our proposal, we will test our framework in a game benchmark and in a chatbot domain. In games, the idea is to learn to play a game and to describe the states and objects of the game, including their dynamics, in simple texts. This description is then transferred to a new game and used to accelerate learning in the new game. Likewise, in chatbots for reservations, for example, the description of objects (elements) that make up the task of restaurant reservation can be used to learn the sequence of interactions in the task of booking hotels, in order to speed-up the solution of this new task.

II. Related Work

A. Transfer and NL

Some work has had successes by using textual description to improve information extraction by a RL agent [15]. Previous work achieved good results towards accelerating the learning speed of RL agents by using transfer techniques that used natural language as a common basis [11], [9]. In these works, as in the current paper, the focus was on devising techniques for the speed-up of the initial reward of a learning agent that was trained and tested in different domains.

B. Object-Oriented MDP

Some research has worked toward convergence speed in RL by embedding the relations between objects in their model. The objects in the domain were classified together with other ones that had similar characteristics. By doing this the relations between two objects of different classes could be used to generalize to other objects of those classes. By using this relations that reduced the dimension of the problem, the authors achieved some training speed improvements[14].

C. Augmenting Transfer Learning with NL using OO-MDP

We extend previous work on the field of transfer learning using NL by incorporating an OO-MDP representation that enhances the generalization of domains trough the relation between objects. The use of OO-MDP approach has been proved successful in reducing the speed of convergence, by using the generalization power of object relations. And so, we will incorporate this OO-MDP representation [14] to some previous models [9], and focus on achieving a better initial reward speed-up when evaluating an agent across domains.

III. Background

The OO-MDP [14] is an extension of the classical MDP and so, we will use the most common MDP notation throughout this paper [13].

A. MDP Notation

The MDP can be represented as a tuple $\langle S, A, T, R, Z\rangle$. We refer as *state* as a unique arrangement of elements in a game scenario, and describe S as the space of all possible states, where the current one is represented as $s \in S$. As A is the set of available *actions* a learning agent can execute, one action of this subset is defined as $a \in A$. The change between states is defined by a *transition function* $T : S \times A \mapsto S$, with $T(s'|s, a)$ as the transition probability of reaching state s' from state s if action a is taken. Also, the *reward function* of reaching a given state is described as $R : S \mapsto \mathbb{R}$ with values as $R(s, a)$. In a *deterministic* MDP, such as the one being considered for this paper, we have that $T(s'|s, a) = 1$. To embed the NL information on the model we use a textual representation Z that describes each element present.

B. Reinforcement Learning (RL)

Given a *scenario* ζ where the agent has a limited number of actions to either achieve its goal state s_g or enter a prohibited state and fail s_f. The ultimate objective of the learning agent is to maximize the accumulated reward in a given scenario. This can be done by using the state-action value function $Q(s, a)$, known as *Q-function*, that is used to determine the reward received after taking action a and being on state s. Now we can define a policy π as the agent commitment of choosing the action that maximizes the value of the *Q-function*, also known as *Q-value*, of the current state: $\pi(s) = \arg\max_a Q(s, a)$. To incorporate the textual representation, we have $\pi(s) = \arg\max_a Q(s, a, Z)$.

To learn an optimal value function, the *Q-learning* technique [16], is often used. Using this technique an agent repeatedly updates the $Q(s, a)$ with the rewards obtained previously. To obtain the optimal Q^*, these updates are use the recursive Bellman equation [1], with the following formulation:

$$Q_{i+1}(s, a, Z) = \mathrm{E}[r + \gamma \max_{a'} Q_i(s', a', Z)|s, a, Z]. \quad (1)$$

Where i indicates the iteration, $r = R(s, a, Z)$ is the immediate reward of the pair s, a, and γ is the discounting factor that applies over the value of future rewards. In this formulation the expectation is applied over all transitions of the s, a pairs.

As a way around the high number of state dimensions the problem can reach, we decided to use a continuous state space where a *deep Q-network* (DQN) [5] could be used to achieve better value than linear function approximators [11]. With this approach the new *Q-function* is written as $Q(s, a; \theta)$, where θ are the coefficients of the approximated function.

C. Textual Representations

The textual representations Z are sentences that describe the characteristics and behavior of certain objects of the scenario being analyzed. For instance, if a object moves, it may have an associated sentence such as "Moves up and down". If the object is static it may be associated with a sentence with the form "Stationary object".

These descriptions are provided in such a way that by being used together, they depicts the current characteristics of the scenario. However it is important to note, that not all elements in the world must have an associated description.

D. OO-MDP Relations

To append the idea of object-oriented to the classical MDP formulation, we consider the relations between objects and their interactions. Given a class c from the set of all classes C, with attributes $\eta \in H$, where H is the set of all attributes, we can say that a object $o \in O$ is an instance of exactly one class: $o \in c$. Any two objects that are interacting in a given state, define a *relation* r between them that occurs at the class level: $r : c \times c \rightarrow Boolean$. By using relations at the class level we can extend the relations between two objects to other ones [14].

IV. Methodology

Consider the following situation to better understand the proposal. For example, in a game with a certain configuration, there may be an object representing an enemy chasing the player. This can be described as "object 1 is an enemy chasing the player". In another game, with another configuration, there may be a different object representing an enemy described in text as "object 2 is a randomly moving enemy". This similar textual description can help a learning agent understand the connection between games more effectively, leading to faster policy learning. It is this fact that we intend to explore in our investigation.

The proposal is that our framework uses both textual descriptions and information regarding the state and action of the source task to learn translation models. These models are embedded in the exploration of policy space in the new learning problem (target task).

We will use public datasets and platforms. Among that, the GVGAI platform has been developed with the main purpose of creating a fair ground for testing and comparing control policies in a video gaming environment [17]. Due to the ease of get going with GVGAI and its environment design simplicity, this platform is quickly becoming a widely used benchmark for testing new RL approaches [18]. Also, the developers of GVGAI hold yearly competitions, where members get to submit their own algorithms for comparison. In this competitions, one of the main characteristics evaluated is the algorithms capability of working in different types of games and scenario. For these aspects, GVGAI was chosen as the best environment for evaluating improvements in transfer learning as well as algorithm adaptability to different scenarios. Finally, there is the benefit of having the models scored on a international ranking.

To evaluate the different models, we consider the following important metrics. First, the average reward, that is the area under the reward curve divided by the number of episodes. Second, the initial performance (or jump start), that is the average reward on the predefined k initial steps. Third, the final performance, that is the average reward on the predefined k final steps. Finally, the decision time and the score on the GVGAI platform will be used as metrics. To run these simulations it will be used the following games: Bomberman, Boulderchase, and Freeway. Bomberman and Boulderchase are very similar games, with very similar rules, goals and dynamics. In both games the agent tries to exit a cave while collecting prizes and avoiding enemies and their attacks. In these games, the agent is also capable of performing attacks. Freeway is a game where the agent tries to cross a road where there are many cars crossing in different paces.

These games were chosen in order to compare transfer learning models with different degrees of game dynamics similarities. On the first scenario, the models will be trained on Bomberman and tested on a version of Bomberman altered on GVGAI, where enemies move faster. On the second scenario, the models will be trained on the Bomberman game, and tested on Boulderchase. On the third scenario, the models will be trained on the Bomberman game, and tested on Freeway. On the fourth and final scenario, the models will be trained on the freeway game and tested on Boulderchase. The idea here is to gradually increase the gap between the game environments and evaluate the learning process speed-up.

Finally, we will give a proof of concept in a scenario of chatbots to book restaurants, theater plays, and hotels. To evaluate the trade-off between decision-making agility and learning speed-up, we will use different combinations of function approximation and textual representation. For the approximation, the linear function and Deep Q-Network (DQN) will be used. For language representation entries, bag-of-words (BOW), bag-of-bigrams (BOB), and long-short-memory (LSTM) will be used.

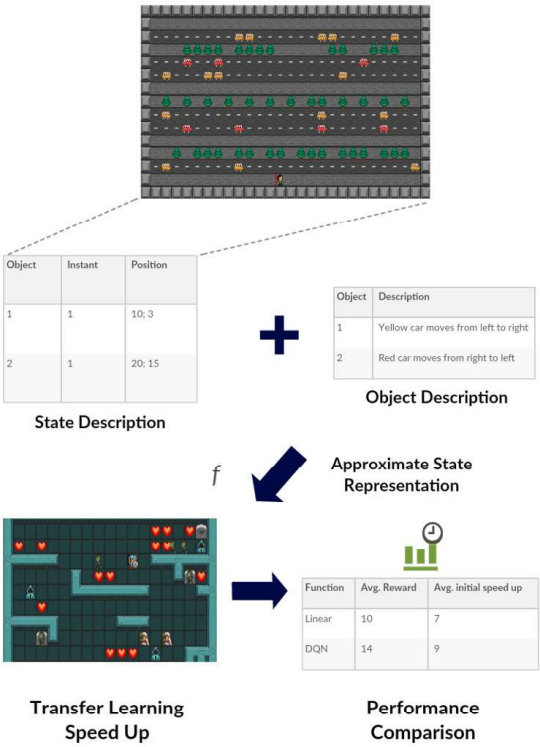


Fig. 1. Visual description of work flow.

For the connection between the reinforcement learning control model and the natural language model, we expect to apply a hybrid top-down bottom-up approach. In this sense, first the agent takes actions and, as it reaches new positions, the reward for that position is used as a training reference for the language representations. After the language models are trained, they will be used in other game scenarios to compare the speed-up of the model convergence. The combinations of these functions and representation entries will be tested and evaluated using the metrics and scenarios described previously.

The general work flow for the methodology and the initial experimental design is displayed in figure 1.

V. Resources and Tools

This investigation will use only public datasets and codes. On the other hand, reinforcement learning requires large computing power from distributed processing units to get results efficiently. In that sense, it should be necessary to use dedicated off-the-shelf computer machines or to access suitable machines in the cloud.

In addition, text descriptions will be crowdsourced using Amazon Mechanical Turk by asking humans to describe entities in video games. However, some descriptions will be written by the research team in order to compare the results, and evaluate how accurate should the descriptions be, in order to achieve satisfatory results.

VI. Conclusion

This scientific research investigation intends to be established as a current reference for the use of texts written in natural language as the basis for the transfer of knowledge between RL tasks. It is expected that there will be a successful increase in transfer learning using the text description. In addition, the most suitable models for each application should be established. We should also be able to get a good score on the GVGAI platform. We should also be able to further enhance the results achieved in previous work, by combining successful approaches.

In terms of applications, this research may lead to new techniques to guide the machine's decision-making based on instructions or textual descriptions of solutions from other tasks. For example, an agent used as a chatbot could learn an optimal general policy to react to user requests based on transcripts of conversations in past interactions. Several other applications in which the automation of a new task can be inspired by solutions of previous tasks can be glimpsed during this research.

Acknowledgment

This work is being carried out with the support of *Itaú Unibanco S.A.*, through the scholarship program of *Programa de Bolsas Itaú* (PBI), linked to the *Centro de Ciência de Dados* (C^2D) of *Escola Politecnica da USP*.

We would like to thank CNPq (Proc. No. 425860 / 2016-7 and N. 307027 / 2017-1), and FAPESP (Proc. N. 2016 / 21047-3) for their support.

References

[1] SUTTON, R. S.; BARTO, A. G. *Reinforcement Learning: An Introduction, unplublished draft*. 2nd. ed. [S.l.: s.n.], 2017.

[2] MITCHELL, T. M. *Machine Learning*. 1st. ed. [S.l.]: McGraw-Hill Education, 1997.

[3] RUSSELL, S.; NORVIG, P. *Artificial Intelligence: A Modern Approach*. 3rd. ed. [S.l.]: Pearson, 2009.

[4] NG, A. Y. et al. Autonomous inverted helicopter flight via reinforcement learning. In: *Experimental Robotics IX*. [S.l.: s.n.], 2006. p. 363–372.

[5] MNIH, V. et al. Human-level control through deep reinforcement learning. *Nature*, v. 518, n. 7540, p. 529–534, 2015.

[6] SILVER, D. et al. Mastering the game of Go without human knowledge. *Nature*, v. 550, n. 7676, p. 354–359, oct 2017. ISSN 0028-0836.

[7] TAYLOR, M. E.; JONG, N. K.; STONE, P. Transferring Instances for Model-Based Reinforcement Learning. In: *Machine Learning and Knowledge Discovery in Databases*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. p. 488–505.

[8] TAYLOR, M. E.; STONE, P. Transfer Learning for Reinforcement Learning Domains: A Survey. *Journal of Machine Learning Research*, v. 10, p. 1633–1685, 2009.

[9] NARASIMHAN, K.; BARZILAY, R.; JAAKKOLA, T. Deep Transfer in Reinforcement Learning by Language Grounding. jul 2017.

[10] KOGA, M. L.; FREIRE, V.; COSTA, A. H. R. Stochastic abstract policies: Generalizing knowledge to improve reinforcement learning. *IEEE Transactions on Cybernetics*, v. 45, n. 1, p. 77–88, 2015.

[11] NARASIMHAN, K.; KULKARNI, T.; BARZILAY, R. Language Understanding for Text-based Games using Deep Reinforcement Learning. In: *Proceedings of the 2015 Conference on Empirical Methods in Natural Language Processing*. Stroudsburg, PA, USA: Association for Computational Linguistics, 2015. p. 1–11. ISBN 9781941643327.

[12] KHOUZAIMI, H.; LAROCHE, R.; LEFEVRE, F. Reinforcement learning for turn-taking management in incremental spoken dialogue systems. In: *IJCAI International Joint Conference on Artificial Intelligence*. [S.l.: s.n.], 2016. v. 2016-Janua, p. 2831–2837. ISBN 9781577357704. ISSN 10450823.

[13] PUTERMAN, M. L. *Markov Decision Processes*. Hoboken, NJ, USA: John Wiley & Sons, Inc., 1994. (Wiley Series in Probability and Statistics). ISBN 9780470316887.

[14] DIUK, C.; COHEN, A.; LITTMAN, M. L. An object-oriented representation for efficient reinforcement learning. In: *Proceedings of the 25th international conference on Machine learning - ICML '08*. New York, New York, USA: ACM Press, 2008. p. 240–247. ISBN 9781605582054.

[15] NARASIMHAN, K.; YALA, A.; BARZILAY, R. Improving Information Extraction by Acquiring External Evidence with Reinforcement Learning. In: *Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing*. Stroudsburg, PA, USA: Association for Computational Linguistics, 2016. p. 2355–2365.

[16] WATKINS, C. J. C. H.; DAYAN, P. Q-learning. *Machine Learning*, v. 8, n. 3-4, p. 279–292, may 1992. ISSN 0885-6125.

[17] PEREZ-LIEBANA, D. et al. General Video Game AI: Competition, Challenges and Opportunities. In: *Thirtieth AAAI Conference on Artificial Intelligence*. [S.l.: s.n.], 2016. p. 4335–4337.

[18] PEREZ-LIEBANA, D. et al. The 2014 General Video Game Playing Competition. *IEEE Transactions on Computational Intelligence and AI in Games*, v. 8, n. 3, p. 229–243, sep 2016. ISSN 1943-068X.

Reinforcement Learning for Mapping Instruction in Natural Language to a Sequence of Actions

DE PAULA, A. M. *†; COSTA, A. H. R. *†
Data Science (C2D) *Center - Escola Politécnica da Universidade de São Paulo
†Laboratory of Intelligent Techniques (LTI) - Escola Politécnica da Universidade de São Paulo
E-mail: {angel.magnossao, anna.reali}@usp.br

***Abstract*—Mapping natural language texts to sequence of actions is challenging because it is essential that commonsense inferences are based on world knowledge. Although there has been work on mapping action scripts, instructions, navigation actions, etc., we present a reinforcement learning approach for automatically mapping instructions from natural language texts to a sequence of actions. The key ideas of our approach are to give leverage to the validation process as the main source of supervision to guide learning as well as not requiring templates in the process of mapping.**

***Keywords*— Natural language processing; Reinforcement Learning.**

***Classification*— Master's degree.**

***Category*— Beginner.**

I. Introduction

Artificial Intelligence (AI) agents will increasingly find assistive roles in homes, labs, factories and public places. The widespread adoption of conversational agents such as Alexa, Siri and Google Home demonstrate the natural demand for such assistive agents [1]. To go beyond supporting the simplistic queries as "How's the weather?", these agents need to be able to dominate domain-specific knowledge such as recipes and other standard operating procedures. While it is possible to hand-code such knowledge (as is done by most of the "skills" used by Alexa-like agents), ultimately that is too labor intensive an option. One way to solve this problem is to have these agents automatically "read" instructional texts, typically written for human workers, and convert them into action sequences and plans for later use [2][3][4].

The problem of interpreting instructions written in natural language has been widely studied since the early days of artificial intelligence [5][6]. In this paper, we present the first steps of reinforcement learning framework development to enable agents to learn autonomously by mapping texts in natural language to a sequence of actions, without any restricted templates. In this and many other applications, the validity of a mapping can be verified by executing the induced actions in the corresponding environment and observing their effects. The key ideas of our approach are to give leverage the validation process as the main source of supervision to guide learning, as well as not requiring templates in the process of mapping. This form of supervision allows us to learn interpretations of natural language instructions when standard supervised techniques are not applicable, because of the lack of human-created annotations [7].

Reinforcement learning (RL) is a natural framework for building models using validation from an environment [8]. We assume that supervision is provided in the form of a reward function that defines the quality of executed actions. During training, the learner repeatedly constructs action sequences for a set of given documents, executes those actions, and observes the resulting reward. The learner's goal is to estimate a policy — a distribution over actions given instruction text and environment state — that maximizes future expected rewards. In the remainder of the paper, we first review previous work related to our approach. After that, we give a formal definition of our plan extraction problem and present our approach in detail, concluding the paper with the next steps of the work.

II. Related work

A. Learning language

Our framework fits into a huge class of approaches that aim to learn language [9][10][11]. Instances of such approaches include work on inferring the meaning of words from video data [12][13], and interpreting the commentary of a simulated soccer game [9]. Most of these approaches assume some form of parallel data, and learn perceptual co-occurrence patterns. In contrast, our emphasis is on learning language by proactively interacting with an external environment.

B. Reinforcement Learning

Reinforcement learning has been previously applied to the problem of dialogue management [14][15][16][17]. These systems converse with a human user by taking actions that emit natural language utterances. The reinforcement learning state space encodes information about the goals of the user and what they say at each time step. The learning problem is to find an optimal policy that maps states to actions, through a trial-and-error process of repeated interaction with the user.

RL is applied very differently in dialogue systems compared to our setup. In some respects, our task is more easily amenable to reinforcement learning. For instance, we are not interacting with a human user, so the cost of interaction is lower. However, while the state space can be designed to be relatively small in the dialogue management task, our state space is determined by the underlying environment and is typically quite large. We address this complexity by applying a policy gradient algorithm that learns efficiently while exploring a small subset of the states.

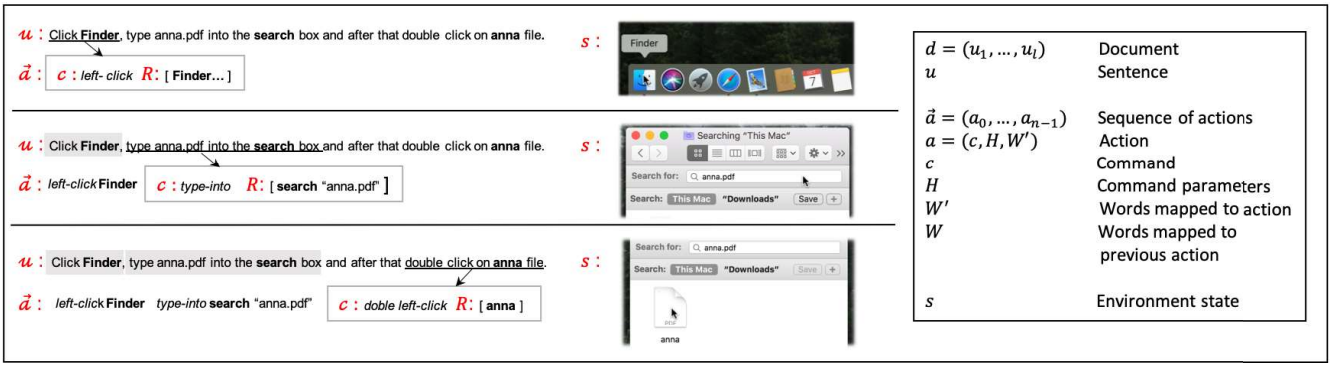


Fig. 1. An example of three-step mapping from an instruction sentence to a sequence of actions. For each step, the figure shows the words selected by the action, along with the corresponding system command and its parameters. The words of W' are underlined, and the words of W are highlighted in grey.

C. *Language Acquisition*

Work has been done on extracting action sequences from action descriptions. For example, [7] proposing a framework to map instructions to sequences of executable actions. [18][19] interpret natural instructions as action sequences or generate navigational action descriptions using an encoder-aligner-decoder structure. Despite the success of these approaches, they all require a limited set of action names given as input, which are mapped to action descriptions. Another approach, proposed by [20], builds action sequences from texts based on dependency parsers and then builds planning models, assuming texts are in restricted templates when describing actions.

In this paper, we aim to extract meaningful action sequences from texts in free natural language, i.e., without any restricted templates, even when the candidate set of actions is unknown.

III. Foundations

In this section, we first describe the task of learning to map between documents and the sequence of actions they express and then introduce the relevant basic concepts of RL

A. *Mapping text to actions*

Having a given document d as input, comprising a sequence of sentences $(u_1, u_2, ..., u_l)$, where each u_i is a sequence of words. Our goal is to map d to a sequence of actions $\vec{a} = (a_1, a_2, ..., a_{n-1})$. Actions are predicted and executed sequentially.

An action $a = (c, H, W')$ encompasses a *command* c, the command's *parameters* H, and the words W' specifying c and H. Elements of H refer to objects available in the environment state, as described below. Some parameters can also refer to words in document d. Additionally, to account for words that do not describe any actions, c can be a null command.

The environment state s specifies the set of objects available for interaction, and their properties. In Figure 1, the environment state s changes in response to the execution of command c with parameters H according to a transition distribution $T(s'|s, c, H)$. This distribution is a priori unknown to the learner.

To predict actions sequentially, we need to track the state of the document-to-actions mapping over time. A *mapping state* ξ is a tuple (s, d, j, W), where s refers to the current environment state; j is the index of the sentence currently being interpreted in document d; and W contains words that were mapped by previous actions for the same sentence. The mapping state ξ is observed after each action.

The initial mapping state s_0 for document d is $(s_d, d, 0, \emptyset)$; s_d is the unique starting environment state for d. Performing action a in state $\xi = (s, d, 0, \emptyset)$ leads to a new state ξ' according to distribution $T(\xi'|\xi, a)$, defined as follows: s transitions according to $T(s'|s, c, H)$, W is updated with a's selected words, and j is incremented if all words of the sentence have been mapped. For the applications in this work, we consider that environment state transitions, and consequently mapping state transitions, are deterministic.

B. *Reinforcement Learning*

Many sequential decision problems are modeled by a Markov Decision Problem (MDP), and RL is an extensively used solution for MDPs. An MDP is described by the tuple $< S, A, T, R >$[21], where S is the set of environment states, A is the set of actions available to an agent, T is the transition function, and R is the reward function, which gives feedback toward task completion.

In the RL framework [8], an agent learns by interacting with an environment over a series of discrete time steps. In each decision step t, the agent observes the current state s_t and applies an action a_t. Then, the next state is defined by a transition probability function T (unknown by the agent in learning scenarios) and the agent receives a reward r_t. The agent's goal in an MDP is to learn an optimal policy π^* that maps each state to the actions that leads to the greatest expected cumulative sum of rewards.

In learning problems (where R and T are unknown) the agent can iteratively learn interacting with the environment, for instance, with the policy gradient algorithm, a function that maps every pair of state and action to an estimate of the long-term reward.

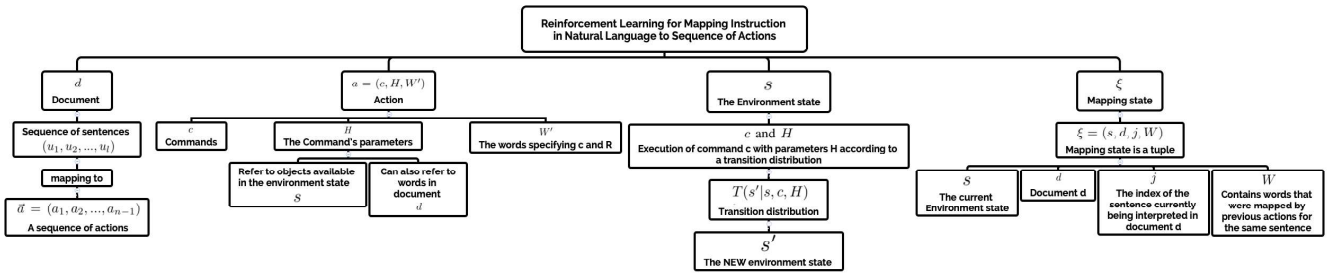


Fig. 2. The overview of our framework showing the fundamental part as build blocks and picturing how each one is formed.

Training

During training, our goal is to find the optimal policy $p(a|\xi;\theta)$. Since reward correlates with correct action selection, a natural objective is to maximize expected future reward — that is, the reward we expect while acting according to that policy from state ξ. Formally, we maximize the value function:

$$V_\theta(s) = E_{p(h|\theta)}[r(h)], \tag{1}$$

where the history h is the sequence of states and actions encountered while interpreting a single document $d \in D$. This expectation is averaged over all documents in D. The distribution $p(h|\theta)$ returns the probability of seeing history h when starting from state ξ and acting according to a policy with parameters θ. This distribution can be decomposed into a product over time steps:

$$p(h|\theta) = \prod_{t=0}^{n-1} p(a_t|t_t;\theta)p(\xi_{t+1}|\xi_t;a_t). \tag{2}$$

A Policy Gradient Algorithm

Our reinforcement learning problem is to find the parameters θ that maximize V_θ from equation 1. Although there is no closed form solution, *policy gradient algorithms* [8] estimate the parameters by performing stochastic gradient ascent. The gradient of V is approximated by interacting with the environment, and the resulting reward is used to update the estimate of θ. Policy gradient algorithms optimize a non-convex objective and are only guaranteed to find a local optimum. However, as we will see, they scale to large state spaces and can perform well in practice.

To find the parameters θ that maximize the objective, we first compute the derivative of V_θ. Expanding according to the product rule, we have:

$$\frac{\partial}{\partial\theta}V_\theta(s) = E_{p(h|\theta)}[r(h)\sum_t \frac{\partial}{\partial\emptyset}\log p(a_t|\xi_t;\theta)], \tag{3}$$

where the inner sum is over all time steps t in the current history h. Expanding the inner partial derivative we observe that:

$$\frac{\partial}{\partial\theta}\log p(a|\xi;\theta) = \phi(\xi,a) - \sum_{a'}\phi(\xi,a')p(a'|\xi;\theta), \tag{4}$$

Equation 4 is easy to compute directly. However, the complete derivative of V_θ in equation 3 is intractable, because computing the expectation would require summing over all possible histories. Instead, policy gradient algorithms employ stochastic gradient ascent by computing a noisy estimate of the expectation using just a subset of the histories. Specifically, we draw samples from $p(h|\theta)$ by acting in the target environment, and use these samples to approximate the expectation. In practice, it is often sufficient to sample a single history h for this approximation.

Algorithm 1 : A policy gradient algorithm.

Input:

A document set D,
Feature representation ϕ,
Reward function $r(h)$,
Number of iterations T.

Initialization:

Set θ to small random values.

Some alg
for $i = 1...T$ **do**
  for each $d \in D$ **do**
    Sample history $h \sim p(h|\theta)$ where
    $h = (\xi_0, a_0, ..., a_{n-1}, \xi_n)$ as fallows:
    for $t = 0...n-1$ **do**
      Sample action $a_t \sim p(a|\xi_t,\theta)$
      Execute a_t on state $\xi_t : \xi_{t+1} \sim p(\xi|\xi_t, a_t)$
    end for
    $\Delta \leftarrow \sum(\phi(\xi_t,a_t) - \sum_{a'}\phi(\xi_t,a')p(a'|\xi_t;\theta))$
    $\theta \leftarrow \theta + r(h)\Delta$
  end for
end for
Output: Estimate of parameters θ.

Algorithm 1 details the complete policy gradient algorithm. It performs T iterations over the set of documents D and samples a history that maps each document to actions. This is done by repeatedly selecting actions according to the current policy, and updating the state by executing the selected actions. The last two lines of the Algorithm compute the empirical gradient and update the parameters.

IV. PROPOSAL

Most of previously proposed methods for interpretation of natural language structions rely on templates in the process of mapping [22][23]. Others as [24][20][25] learn sentence patterns and lexicons or use using NLP tools. These tools are trained for universal natural language processing tasks, they cannot solve the complex action sequence extraction problem well [1].

The key ideas of our work are to leverage the process of validation as a main strain of return for guiding the process of learning. Moreover, not requiring templates in the process of mapping. To understand our framework we can count on Figure 2, it gives us an overview of the whole instrution, showing the fundamental parts as build blocks and how each one is formed. The goal is to predict a sequence of actions $\vec{a} = (a_1, ..., a_{n-1})$. We construct this sequence by repeatedly choosing an action a given the current mapping state $\xi = (s, d, j, W)$, and applying that action a to advance to a new state ξ'. Given a state ξ' the space of possible next actions is defined by enumerating subspans of unused words in the current sentence (i.e., subspans of the jth sentence of d not in W), and the possible commands and parameters in environment state s.

V. CONCLUSION

In this paper, we presented a reinforcement learning approach for automatically mapping instructions from texts to a sequence of actions. In the next steps, we will investigate different configurations of state and actions as well as the most appropriate RL algorithm to solve the problem. Comparative analysis with different options will be carried out in order to find the best options for our framework.

ACKNOWLEDGMENT

This work was carried out with the support of Itaú Unibanco S.A., through the Itaú Scholarship Program (PBI), linked to the Data Science Center (C2D) of the Escola Politécnica da Universidade de São Paulo. We are also grateful for the Escola de Engenharia de Computação da Escola Politécnica da Universidade de São Paulo for providing room for the development of the field of artificial intelligence and machine learning, through the Laboratory of Intelligent Techniques (LTI). We would like to thank CNPq (Proc. No. 425860 / 2016-7 and N. 307027 / 2017-1), and FAPESP (Proc. N. 2016 / 21047-3) for their support.

REFERENCES

[1] FENG, W.; ZHUO, H. H.; KAMBHAMPATI, S. Extracting action sequences from texts based on deep reinforcement learning. *arXiv preprint arXiv:1803.02632*, 2018.

[2] ZHUO, H. H.; YANG, Q. Action-model acquisition for planning via transfer learning. *Artificial intelligence*, Elsevier, v. 212, p. 80–103, 2014.

[3] ZHUO, H. H.; MUÑOZ-AVILA, H.; YANG, Q. Learning hierarchical task network domains from partially observed plan traces. *Artificial intelligence*, Elsevier, v. 212, p. 134–157, 2014.

[4] ZHUO, H. H.; KAMBHAMPATI, S. Model-lite planning: Case-based vs. model-based approaches. *Artificial Intelligence*, Elsevier, v. 246, p. 1–21, 2017.

[5] WINOGRAD, T. Understanding natural language academic press, ny. 1973.

[6] EUGENIO, B. D. Understanding natural language instructions: the case of purpose clauses. In: ASSOCIATION FOR COMPUTATIONAL LINGUISTICS. *Proceedings of the 30th annual meeting on Association for Computational Linguistics*. [S.l.], 1992. p. 120–127.

[7] BRANAVAN, S. R. et al. Reinforcement learning for mapping instructions to actions. In: ASSOCIATION FOR COMPUTATIONAL LINGUISTICS. *Proceedings of the Joint Conference of the 47th Annual Meeting of the ACL and the 4th International Joint Conference on Natural Language Processing of the AFNLP: Volume 1-Volume 1*. [S.l.], 2009. p. 82–90.

[8] SUTTON, R. S. et al. *Reinforcement learning: An introduction*. [S.l.]: MIT press, 1998.

[9] CHEN, D. L.; MOONEY, R. J. Learning to sportscast: a test of grounded language acquisition. In: ACM. *Proceedings of the 25th international conference on Machine learning*. [S.l.], 2008. p. 128–135.

[10] MOONEY, R. J. Learning language from its perceptual context. In: SPRINGER. *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*. [S.l.], 2008. p. 5–5.

[11] FLEISCHMAN, M.; ROY, D. Intentional context in situated natural language learning. In: ASSOCIATION FOR COMPUTATIONAL LINGUISTICS. *Proceedings of the Ninth Conference on Computational Natural Language Learning*. [S.l.], 2005. p. 104–111.

[12] ROY, D. K.; PENTLAND, A. P. Learning words from sights and sounds: A computational model. *Cognitive science*, Wiley Online Library, v. 26, n. 1, p. 113–146, 2002.

[13] BARNARD, K.; FORSYTH, D. Learning the semantics of words and pictures. In: IEEE. *Computer Vision, 2001. ICCV 2001. Proceedings. Eighth IEEE International Conference on*. [S.l.], 2001. v. 2, p. 408–415.

[14] SCHEFFLER, K.; YOUNG, S. Automatic learning of dialogue strategy using dialogue simulation and reinforcement learning. In: MORGAN KAUFMANN PUBLISHERS INC. *Proceedings of the second international conference on Human Language Technology Research*. [S.l.], 2002. p. 12–19.

[15] ROY, N.; PINEAU, J.; THRUN, S. Spoken dialogue management using probabilistic reasoning. In: ASSOCIATION FOR COMPUTATIONAL LINGUISTICS. *Proceedings of the 38th Annual Meeting on Association for Computational Linguistics*. [S.l.], 2000. p. 93–100.

[16] LITMAN, D. J. et al. Automatic optimization of dialogue management. In: ASSOCIATION FOR COMPUTATIONAL LINGUISTICS. *Proceedings of the 18th conference on Computational linguistics-Volume 1*. [S.l.], 2000. p. 502–508.

[17] SINGH, S. P. et al. Reinforcement learning for spoken dialogue systems. In: *Advances in Neural Information Processing Systems*. [S.l.: s.n.], 2000. p. 956–962.

[18] MEI, H.; BANSAL, M.; WALTER, M. R. Listen, attend, and walk: Neural mapping of navigational instructions to action sequences. In: *AAAI*. [S.l.: s.n.], 2016. v. 1, p. 2.

[19] DANIELE, A. F.; BANSAL, M.; WALTER, M. R. Navigational instruction generation as inverse reinforcement learning with neural machine translation. In: ACM. *Proceedings of the 2017 ACM/IEEE International Conference on Human-Robot Interaction*. [S.l.], 2017. p. 109–118.

[20] LINDSAY, A. et al. Framer: Planning models from natural language action descriptions. 2017.

[21] PUTERMAN, M. L. *Markov decision processes: discrete stochastic dynamic programming*. [S.l.]: John Wiley & Sons, 2014.

[22] FIKES, R. E.; NILSSON, N. J. Strips: A new approach to the application of theorem proving to problem solving. *Artificial intelligence*, Elsevier, v. 2, n. 3-4, p. 189–208, 1971.

[23] POMARLAN, M.; KORALEWSKI, S.; BEETZ, M. From natural language instructions to structured robot plans. In: SPRINGER. *Joint German/Austrian Conference on Artificial Intelligence (Künstliche Intelligenz)*. [S.l.], 2017. p. 344–351.

[24] SIL, A.; HUANG, F.; YATES, A. Extracting action and event semantics from web text. In: *AAAI Fall Symposium: Commonsense Knowledge*. [S.l.: s.n.], 2010.

[25] SIL, A.; YATES, A. Extracting strips representations of actions and events. In: *Proceedings of the International Conference Recent Advances in Natural Language Processing 2011*. [S.l.: s.n.], 2011. p. 1–8.

ARTIGOS DE DOUTORADO

Data Lake architectural model based on files and metadata

Modelo Arquitetural de Data Lake centrado em arquivos e metadados

MENDES, E.M..[*]; ALMEIDA JR, J.R.[*]
[*]Laboratório de Ciências - Universidade de São Paulo
[†]Laboratório de Processamento de Sinais - Escola de Engenharia de Computação
{eduardo.marreto, jorgerady}@usp.br

***Abstract*— The Data Lake concept arises based on organizational challenge of data centralization in a unique structure for knowledge extraction. However, data storage and read performance considering large data volume, requires optimized strategies. In this context, it is presented the approach of binary files as data repository, being described three main possibilities: Apache Parquet, Apache Avro and Apache ORC. Other key practice presented is the use of metadata for data semantic analysis, data quality analysis, data lineage and fill requirements about legal norms and restrictions.**

***Keywords*— data lake, big data, data science, binary files, metadata.**

Resumo*— Dado o desafio de centralizar todos os dados organizacionais em uma estrutura única para extração de conhecimento, surge o conceito de Data Lake. Porém, o armazenamento considerando grandes volumes de dados, bem como a recuperação e extração de informações, exigem a utilização de mecanismos otimizados. Como proposta apresentada, utiliza-se para armazenamento de dados estruturas de arquivos binários, sendo caracterizados três principais tipos, Apache Parquet, Apache Avro e Apache Orc. Além do armazenamento, faz-se necessário construir abordagem de metadados para obtenção da semântica da informação, bem como a criação de marcadores de qualidade, visando orientar a linhagem do dado, além de suportar o cumprimento de normas e restrições legais.*

***Palavras-chave*— data lake, big data, ciência de dados, arquivos binários, metadados.**
Classificação — Doutorado.
Categoria — iniciante

I. Introdução

O termo *Big Data* é associado a diversos desafios técnicos e de governança. À medida que as organizações estruturam processos de coleta e processamento de dados, surgem então possíveis silos de dados, que podem estar completamente desassociados, possuindo diferentes estruturas, formatos e volumes, dificultando assim a extração de conhecimento. É neste cenário que é proposta a estrutura de *Data Lake [1],* uma abordagem de repositório centralizado de *Big Data* que unifica os dados brutos coletados.

II. Data Lake

Englobando as características de Big Data como grande volume de dados, velocidade e variedade de formatos - com dados estruturados, semi-estruturados e não estruturados - e, considerando o aparecimento de ferramental do ecossistema Hadoop, construiu-se então uma nova arquitetura para estruturas analíticas, denominado *Data Lake* [2].

Em sua primeira definição, realizada por James Dixon [3], *Data Lake* foi definido como uma estrutura em que: "Se você pensar em um Data Mart como uma garrafa de água - limpa, embalada e estruturada para fácil consumo - o Data Lake é onde a água se encontra em seu estado mais natural. O conteúdo provém de diversas origens e vários usuários do lago podem examinar, mergulhar ou colher amostras da água".

Enquanto as estruturas analíticas de *Data Warehouse* e *Data Mart* se concentram em indicadores conhecidos e dimensões pré-definidas, o *Data Lake* concentra-se em englobar todo o volume de dados corporativos, movendo-os para uma mesma estrutura física baseado em ferramentas Hadoop, e visando futuras inferências sobre o dado [2]. Por não se limitar a dados estruturados, possuir múltiplas origens de dados e englobar maior questionamento dos dados, *Data Lake* pode se direcionar para inovação e descobertas [4].

Porém o armazenamento, considerando grandes volumes de dados, bem como a recuperação e extração de informações, exigem a utilização de mecanismos otimizados, sendo a estrutura de arquivos binários uma abordagem relevante. E, a medida que aumentam os volumes de dados armazenados no Data Lake, com diversas origens e formatos, torna-se relevante a utilização de metadados apropriados para a extração de informações. A não aplicação de metadados em todas as fases do repositório podem impossibilitar o uso e extração de conhecimento, impactando na agilidade de análises [10], criando "Pântanos de dados".

III. *Arquivos binários como repositório de dados*

Arquivos binários englobam formatos de arquivos otimizados para o armazenamento e recuperação de dados, principalmente quando comparados a estruturação não binárias, como JSON, XML ou CSV [16]. Suas implementações incluem diferentes estratégias de armazenamento, e de maneira comum, para cada arquivo, aplicam o uso de esquemas (schemas) de dados e compressão de volume de dados. Dentre os formatos utilizados de arquivos binários, destacam-se: Apache Parquet, Apache Avro e Apache ORC.

A seleção do formato apropriado de arquivo depende do formato de origem da informação e compatibilidade com ferramentas de armazenamento e recuperação de dados.

A. *Apache Parquet*

Os arquivos Apache Parquet são baseados em estrutura colunar, possuem schema e utilizam mecanismo de compressão, possuindo compatibilidade com projetos do ecossistema Hadoop [5].

A sua estrutura colunar é composta da estrutura de colunas associadas a chunks de dados, bem como o uso de metadados. A figura 1 ilustra a estrutura lógica do Arquivo Apache Parquet.

Fig.1. Estrutura de arquivo parquet

```
4-byte magic number "PAR1"
<Coluna 1 Chunk 1 + Metadado da Coluna>
<Coluna 2 Chunk 1 + Metadado da Coluna>
...
<Coluna N Chunk 1 + Metadado da Coluna>
<Coluna 1 Chunk 2 + Metadado da Coluna>
<Coluna 2 Chunk 2 + Metadado da Coluna>
...
<Coluna N Chunk 2 + Metadado da Coluna>
...
<Coluna 1 Chunk M + Metadado da Coluna>
<Coluna 2 Chunk M + Metadado da Coluna>
...
<Coluna N Chunk M + Metadado da Coluna>
Metadado do arquivo
4-byte tamanho em bytes do metadado do arquivo
4-byte magic number "PAR1"
```

(fonte: traduzido de PARQUET [5])

Nota-se que em sua estrutura há a aplicação de metadados no nível de coluna e arquivo, bem como o agrupamento de linhas, definido como chunks.

B. *Apache Avro*

Os arquivos Apache Avro possuem schema de dados baseados em formato JSON e utilizam mecanismo de compactação para o armazenamento de dados em forma persistente [6].

Dado que sua estrutura é baseada em JSON, permite o armazenamento de tipos complexos de dados, ou seja, objetos compostos por objetos. A figura 2 ilustra uma estrutura composta de tipos complexos passível de armazenamento em AVRO.

Fig.2. Exemplo de estrutura AVRO

```
{
    "tipo": "registro",
    "nome": "teste",
    "campos" : [
            {"nome": "a", "tipo": "long"},
            {"nome": "b", "tipo": "string"}
        ]
}
```

(fonte: traduzido de AVRO [6])

Nota-se que em sua estrutura, que o registro descrito possui três atributos: “tipo”, “nome” e “campos”. O atributo “campos” é definido como complexo, possuindo dois outros atributos, “nome” e “tipo”.

C. *Apache ORC*

Apache ORC é um formato nativo do ecossistema Hadoop, criado em 2013, e que possui foco na velocidade de processamento e compactação de volume de dados [7].

Sua estrutura é colunar e utiliza mecanismo de compactação. O formato ORC provê diferentes níveis de indexação de dados, sendo eles [7]:

- Nível de arquivo: estatísticas sobre os valores em cada coluna para todo o arquivo;
- Nível de faixa: estatísticas sobre valores de uma faixa de colunas;
- Nível de linha: estatísticas sobre valores de cada coluna para conjunto de 10 mil linhas em uma faixa;

As estatísticas associadas aos índices visam aumentar o desempenho de buscas de dados nos arquivos, visto que os registros podem ser agrupados por faixas, tendo com base os valores dos atributos representados nas colunas.

IV. *Metadados*

Data Lake pode direcionar companhias à inovação e descobertas [4] e arquivos formatados representam estratégias eficientes de armazenamento de dados [8]. Porém apenas esta abordagem não garante uma prática eficaz de estrutura analítica.

Estudos de mercado do Gartner [9] indicam que mais de 80% dos dados corporativos são não estruturados, e de acordo com pesquisas da IBM, estima-se que mais de 70% do tempo em projetos de Analytics são relacionados com a identificação, limpeza e localização de dados nas estruturas. A proposição de um Data Lake apenas com dados “crus”, sem tratamento, não aumenta a agilidade e acessibilidade do dado, visto que boa

parte do trabalho de preparação do dado é postergado para a fase de consumo [10].

Para apoiar o consumo e gestão dos dados, faz-se válida a abordagem de construção de metadados aos arquivos do Data Lake. Hai et.al. [1] definem que há necessidade de extrair o máximo possível de metadados durante a fase de ingestão, e que sem a utilização de metadados, a utilização de dados no Data Lake é difícil, tornando as estruturas semânticas desconhecidas, o que transforma o "Lago de dados" em um "Pântano de dados".

Além das preocupações quanto à semântica da informação, a aplicação de metadados auxilia quanto a gestão do Data Lake, pois apoiam a criação de marcadores de qualidade, orientam quanto a linhagem do dado ("*Data Lineage*") e suportam ao cumprimento de normas e restrições legais [11].

Os metadados designados como apoio a marcadores de qualidade de dados devem endereçar as dimensões de qualidade requisitadas no contexto da análise de dados. Como direcionador, utiliza-se as dimensões referenciadas por Firmani [12], sendo elas: acurácia, completude, consistência, redundância, legibilidade, acessibilidade, veracidade e utilidade.

A linhagem provê uma visão do repositório não somente como um conjunto isolado de entidades, mas sim como um conjunto que pode ter origem a partir de agregações de múltiplos datasets e que, por meio de rotinas de transformações, podem gerar diversos outros datasets. A visão de linhagem, bem como a rastreabilidade, quando oferecidas como metadados, auxiliam usuários em um melhor entendimento do conteúdo do Data Lake [13].

Já as normas e restrições legais ganharam uma alta relevância nos últimos anos, principalmente por leis regulatórias como o GDPR [14] e lei de proteção de dados no Brasil. Estas normas englobam requisitos complexos como, a partir de solicitações de usuários, efetuar remoção de dados [15], a identificação de dados sensíveis, bem como a análise de rastreabilidade é apoiada pela aplicação de metadados no Data Lake.

A) *Metadados em arquivos binários*

Para as três opções apresentadas, Apache Parquet, Apache AVRO e Apache Orc, nota-se a aplicação de metadados referentes ao schema dos dados contidos e metadados de estatísticas dos dados em níveis de linha e colunas.

A disposição destes metadados "esquemáticos" apoiam o entendimento, descoberta e utilização dos dados, e é fundamental na fase de tratamento de dados [10].

V. Conclusão

A partir das referências apresentadas, nota-se a importância de definição de estratégia para armazenamento de dados e a utilização de metadados adequados em arquitetura analítica Data Lake.

A seleção adequada de formato para repositório em arquivos binários, considerando a natureza do dado e compatibilidade com ferramentas utilizadas, permite uma abordagem escalável, com capacidade de compressão e alto desempenho em recuperação de dados.

Além disso, arquivos binários possuem nativamente em suas estruturas metadados esquemáticos, que definem as estruturas dos dados e, associados a metadados de gestão, permitem um abordagem de Data Lake que propicia a utilização e extração de informações.

Referências

[1] HAI, R.; GEISLER, S.; QUIX, C. Constance: An Intelligent Data Lake System. Proceedings of the International Conference on Management of Data, p. 2097–2100, 2016.

[2] MADERA, C.; LAURENT, A. The next information architecture evolution. Proceedings of the 8th International Conference on Management of Digital EcoSystems - MEDES, p. 174–180, 2016.

[3] DIXON, J. Pentaho, Hadoop, and Data Lakes, 2010, Disponível em: https://jamesdixon.wordpress.com/2010/10/14/pentaho-hadoop-and-data-lakes/. Acesso em: 01 de Jun. 2018.

[4] O'LEARY, D. E. Embedding AI and crowdsourcing in the big data lake. IEEE Intelligent Systems, v. 29, n. 5, p. 70–73, 2014.

[5] APACHE PARQUET. Disponível em: http://parquet.apache.org/documentation/latest/ . Acesso em: 01 de Out. 2018.

[6] APACHE AVRO. Disponível em: http://avro.apache.org/docs/current/ . Acesso em: 01 de Out. 2018.

[7] APACHE ORC. Disponível em: https://orc.apache.org/docs/ . Acesso em: 01 de Out. 2018.

[8] AHMED, S. et al. Modern Data Formats for Big Bioinformatics Data Analytics. IJACSA International Journal of Advanced Computer Science and Applications, v. 8, n. 4, p. 366–377, 2017.

[9] GARTNER. Organizations Will Need to Tackle Three Challenges to Curb Unstructured Data Glut and Neglect. 17. Jun, 2015.

[10] TERRIZZANO, I. et al. Data Wrangling: The Challenging Journey from the Wild to the Lake. 7th Biennial Conference on Innovative Data Systems Research CIDR'15, 2015.

[11] MATHIS, C. Data Lakes. Datenbank-Spektrum, 2017.

[12] FIRMANI, D. et al. On the Meaningfulness of "Big Data Quality" (Invited Paper). Data Science and Engineering, v. 1, n. 1, p. 6–20, 2016.

[13] HALEVY, A. et al. Managing Google's data lake: an overview of the Goods system. Bulletin of the technical committee on Data Engineering IEEE Computer Society, v.39, n.3., Set., 2016.

[14] MARTIN, Y.-S.; KUNG, A. Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), p. 108–111, 2018.

[15] KUHN, D. R. A Data Structure for Integrity Protection with Erasure Capability. n. May, 2018.

[16] SHARMA, K.; MARJIT, U.; BISWAS, U. Efficiently Processing and Storing Library Linked Data using Apache Spark and Parquet. Information Technology and Libraries, v. 37, n. 3, p. 29, 2018.

Improving the quality of scientific software through usability
Melhoria na qualidade do software científico por meio da usabilidade

CONTESSOTO, A. G*; ALMEIDA JR, J.R.*;
*School of Electrical and Computer Engineering
E-mail: {contessoto, jorgerady}@usp.br

***Abstract*—The development of scientific research is linked to the use of software. In spite of this, the development of scientific software results in low-quality products since the developers are the researchers who know the application methodology, but who do not know or do not apply software engineering techniques. The lack of quality in scientific software is mainly reflected in usability issues, such as ease of use and way of visualizing information. In this sense, the project aims to improve usability in scientific software by means of a set of exclusive heuristics to this type of software, in order to assist the researchers that develop their own software. In addition, a usability evaluation mechanism will be created for scientific software in order to evaluate the quality of usability of the software in development and of those that already exist. As scientific software covers different areas, bioinformatics softwares will be used as proof of concept, since its community is already concerned about the way in which such software is constructed. Thus, for an evaluation of the heuristics, prototypes of bioinformatics software will be constructed, which will be evaluated in two empirical evaluations, with the help of developers and users, and in a comparative evaluation, using the main general usability references.**

***Keywords*— Usability; Scientific Software; Quality; Bioinformatics.**

***Resumo*— O desenvolvimento de pesquisas científicas está ligado à utilização de softwares. Apesar disso, o desenvolvimento de softwares científicos resulta em produtos de baixa qualidade, uma vez que os desenvolvedores são os próprios pesquisadores que detêm um conhecimento amplo sobre o domínio da aplicação, mas que, em contrapartida, não conhecem ou não aplicam técnicas de engenharia de software. A falta de qualidade nos softwares científicos se reflete principalmente nos quesitos de usabilidade, como, por exemplo, facilidade de uso e forma de visualização das informações. Nesse sentido, a pesquisa tem como objetivo melhorar a usabilidade em softwares científicos por meio de um conjunto de heurísticas exclusivas para esse tipo de software, de modo a auxiliar os pesquisadores que desenvolvem seus próprios softwares. Além disso, será criado um mecanismo de avaliação de usabilidade para os softwares científicos, de modo a avaliar a qualidade da usabilidade dos softwares em desenvolvimento e dos já existentes. Como os softwares científicos abrangem diferentes áreas, serão utilizado como prova de conceito softwares de bioinformática, uma vez que a comunidade já demonstra preocupação com a maneira como tais softwares são construídos. Assim, para a avaliação das heurísticas, serão construídos protótipos de softwares de bioinformática que serão considerados em duas avaliações empíricas, que contarão com o auxílio de desenvolvedores e usuários, e uma avaliação comparativa, utilizando os principais benchmarks gerais de usabilidade.**

***Palavras-chave*— Usabilidade; Software Científico, Qualidade, Bioinformática.**

***Classificação*— Doutorado**

***Categoria*— Iniciante**

I. Introdução

O desenvolvimento de qualquer pesquisa científica está fortemente ligado à utilização de softwares, que auxiliam desde tarefas gerais, como a criação do texto de uma publicação, até tarefas específicas de certos domínios, como a contagem de cadeias de DNA semelhantes em uma amostra. Nesse sentido, os softwares que auxiliam tarefas gerais são criados com um escopo mais amplo, de modo a buscar servir o maior número de pessoas [1]. Por sua vez, os softwares científicos, que auxiliam tarefas específicas de um domínio, são muitas vezes desenvolvidos por pessoas que detêm um grande conhecimento teórico e experiência no estudo do domínio, mas que, em contrapartida, têm pouco conhecimento das técnicas e das boas práticas de engenharia de software [2], [3], [4]. Como consequência, os softwares científicos apresentam falhas de qualidade, principalmente no que diz respeito à usabilidade e à sua manutenção [5], [4].

A qualidade no desenvolvimento de software consiste na criação de um produto útil que forneça valor mensurável para as partes interessadas no produto final [6]. Um produto útil é aquele que contempla o conteúdo, as funções e os recursos acordados, de modo a fornecer confiabilidade e segurança nos resultados [1], [6].

O termo usabilidade começou a ser utilizado em 1985, a partir do trabalho de Gould e Lewis [7]. Com o passar dos anos, surgiram inúmeras definições para o conceito. O IEEE define usabilidade como sendo a facilidade com que um usuário pode aprender a operar, preparar entradas e interpretar saídas de um sistema ou componente [8]. Por sua vez, o padrão ISO/IEC 9241 define a usabilidade como a extensão em que um produto pode ser usado por um grupo de usuários, com o intuito de atingir metas específicas com efetividade, eficiência e satisfação em um contexto de uso [9]. De acordo com Madan

e Dubey (2012), a usabilidade é um atributo de um produto que infuencia a qualidade de um sistema de software [10].

De acordo com as definições apresentadas, o conceito de usabilidade não trata apenas da beleza ou da facilidade de uso de uma interface de software, o que geralmente é pensado pelos usuários e desenvolvedores de softwares, mas sim o quão bem os usuários podem interagir com uma tecnologia, de modo a realizar com êxito as atividades atribuídas, atingindo os objetivos pretendidos de forma satisfatória. Assim, é possível afirmar que a usabilidade é um atributo relevante para a análise de qualidade de um produto de software [11].

O processo de avaliação da usabilidade desempenha um papel fundamental na interação humano-computador, uma vez que busca detectar problemas na maneira como o usuário e o sistema se relacionam e pode ser executado em qualquer fase do processo de desenvolvimento de software. O método de avaliação de usabilidade mais utilizado é a avaliação heurística, proposta por Jakob Nielsen. O método consiste em um grupo de avaliadores de usabilidade analisar o software a partir de um conjunto de heurísticas definidas, com o objetivo de detectar problemas de usabilidade no software [12]. Nielsen propõe um conjunto de dez heurísticas de usabilidade, que são as mais aceitas por pesquisadores e pela indústria [13]. Apesar da relevância, as dez heurísticas são consideradas muito gerais para serem aplicadas em todos os tipos de software. Nesse sentido, outras propostas surgiram com o intuito de suprir características específicas de diferentes domínios, utilizando as heurísticas de Nielsen como base [14], [4].

O presente trabalho de doutorado tem o intuito de melhorar a qualidade na usabilidade em softwares científicos, por meio de um conjunto de heurísticas de usabilidade específicas para esse tipo de software, de modo a auxiliar os desenvolvedores durante o processo de desenvolvimento e os usuários durante a utilização desses softwares. Dessa forma, o presente artigo tem o intuito de apresentar o contexto de usabilidade em softwares científicos, bem como expor o método de pesquisa a ser empregado durante a execução do projeto.

II. Usabilidade em softwares científicos

A usabilidade é um quesito fundamental para a qualidade de softwares, principalmente quando tais softwares são utilizados para a realização de uma tarefa específica. Assim, a presença de usabilidade em softwares científicos é essencial para que os softwares consigam auxiliar de forma efetiva a realização de tarefas. No contexto de pesquisas na área biológica, desde a conclusão do projeto do genoma humano, softwares se tornaram indispensáveis para a área. Assim, a bioinformática surgiu como um campo de pesquisa interdisciplinar, reunindo várias áreas como biologia molecular, bioquímica, física biológica, engenharia elétrica, ciência da computação, dentre outras. Nesse sentido, a bioinformática pode ser definida como sendo qualquer aplicação de métodos computacionais para a resolução ou simulação de problemas biológicos [15]. A partir dos anos 2000, muitos softwares de bioinformática foram criados, com o intuito de dar suporte à pesquisa científica, sendo que a comunidade concentra esforços no desenvolvimento de métodos computacionais e estatísticos que buscam simular o comportamento de sistemas biológicos [16].

Apesar disso, surge a preocupação na comunidade de como esses softwares são desenvolvidos. Ainda são poucos os estudos que demonstram cuidado com a forma de desenvolvimento dos softwares de bioinformática e com a qualidade desses softwares. Dessa forma, a discussão é relevante e ganha destaque, pois, muitas vezes, os pesquisadores passam mais tempo lidando com a complexidade do desenvolvimento e resolvendo falhas nos softwares do que com a resolução do problema científico em si, o que é resultado da não utilização de técnicas de engenharia de software no desenvolvimento desses softwares [17], [11], [4].

O estudo realizado por Umarji et al. (2009) aponta que metade dos desenvolvedores de softwares de bioinformática fazem parte do grupo de usuários finais do software, ou seja, são os pesquisadores de áreas específicas, como a biologia e a física, que desenvolvem seus próprios softwares. O estudo contou com uma amostragem de 126 participantes, membros de grupos de estudos de bioinformática da América do Norte e da Europa. Outro resultado de destaque é o fato de os participantes afirmarem que a usabilidade, a confiabilidade, a manutenção e a qualidade geral dos softwares eram insatisfatórios [18]. Esses resultados comprovam a necessidade da aplicação de técnicas para a obtenção de qualidade nos softwares de bioinformática, que considerem o fato de os desenvolvedores não terem uma formação formal para o desenvolvimento de software.

Assim, observa-se que os softwares científicos são desenvolvidos, na maior parte dos casos, por pesquisadores que não detêm conhecimento a respeito de boas práticas para o desenvolvimento de software, principalmente no que diz respeito à usabilidade. Esse fato ocorre, dentre outros fatores, pela formação acadêmica dos pesquisadores. Como consequência, os softwares científicos apresentam baixa qualidade, o que dificulta a divulgação de tais softwares e a utilização por outros pesquisadores de áreas correlatas. Portanto, para auxiliar os pesquisadores a desenvolverem softwares científico com qualidade na usabilidade, é necessária a utilização de heurísticas de usabilidade específica para softwares científicos, que sejam simples de serem aplicadas e entendidas por pesquisadores que tenham diferentes formações.

Como a comunidade científica é ampla, faz-se necessária a escolha de um domínio específico de software para aplicar as heurísticas e comprovar a sua eficácia. Dessa forma, foi escolhida a bioinformática, uma vez que a comunidade da área já apresenta uma preocupação na forma segundo a qual os softwares de bioinformática estão sendo desenvolvidos e já identificaram a necessidade de seguirem padrões de desenvolvimento.

III. Método de pesquisa

O método a ser empregado no projeto baseia-se na ideia inicial de identificar o perfil dos desenvolvedores de softwares científicos, de modo a dividir aqueles que realizam seus trabalhos no Brasil ou no exterior e também aqueles que

trabalham especificamente com softwares de bioinformática, com o intuito de identificar as características particulares dos membros de cada grupo. A identificação do perfil é relevante, uma vez que as heurísticas devem considerar as características particulares dos desenvolvedores que as utilizarão.

Posteriormente, serão definidas as heurísticas de usabilidade para os softwares científicos, baseando-se nas heurísticas mais relevantes encontradas na literatura e considerando as características particulares dos softwares científicos. Após a definição das heurísticas, será definido o mecanismo de avaliação da usabilidade para softwares científicos, considerando os principais benchmarks gerais de usabilidade disponíveis na literatura. Após essa etapa, serão desenvolvidos protótipos de softwares de bioinformática já existentes, utilizando como base as heurísticas criadas. Tais protótipos serão utilizados durante o processo de avaliação das heurísticas.

Após a criação dos protótipos, ocorrerá o processo de avaliação das heurísticas. Esse processo será dividido em três etapas, a saber: avaliação empírica dos desenvolvedores, avaliação empiríca dos usuários e avaliação comparativa. Para a avaliação empírica dos desenvolvedores, serão utilizados os grupos de desenvolvedores previamente identificados, de modo a considerar a opinião deles a respeito da utilização das heurísticas e do resultado final de usabilidade gerado nos softwares. Já para a avaliação comparativa, será realizada a comparação dos protótipos desenvolvidos com as versões originais dos softwares de bioinformática, sendo realizada a avaliação por meio do mecanismo de avaliação criado e com os principais benchmarks da literatura. Por fim, para a avaliação empírica dos usuários, serão convidados usuários de softwares de bioinformática, para que eles utilizem os protótipos e as versões originais dos softwares de bioinformática e, após a utilização, deem a opinião a respeito da sua experiência com os sistemas, considerando os critérios de usabilidade. Após a avaliação, caso necessário, ocorrerá um refinamento das heurísticas, considerando os resultados das três avaliações.

Por fim, será desenvolvido um framework das heurísticas, que auxiliará a aplicação do conjunto de heurísticas de usabilidade, independente da formação acadêmica e experiências dos desenvolvedores. É importante destacar que durante a execução do projeto, artigos científicos serão produzidos para divulgar os resultados, na medida em que eles forem alcançados.

IV. Análise dos resultados

Para a análise dos resultados foram escolhidos, como prova de conceitos, softwares de bioinformática, uma vez que softwares desse tipo específico representam uma parcela de softwares científicos e a comunidade de bioinformática já demonstra preocupação com a forma de desenvolvimento de seus softwares. Assim, as heurísticas de usabilidade para softwares científicos serão avaliadas a partir de aplicações de bioinformática, levando em consideração três etapas distintas, a saber: avaliação empírica dos desenvolvedores, avaliação empírica dos usuários e avaliação comparativa. Para a avaliação comparativa e a avaliação empírica dos usuários, serão construídos protótipos de softwares de bioinformática que estejam em uso, tomando como base as heurísticas de usabilidade criadas.

Para a avaliação empírica dos desenvolvedores, os grupos identificados previamente serão divididos em dois grupos de estudo. Os participantes do primeiro grupo de estudo receberão a tarefa de desenvolver um protótipo de software de bioinformática, considerando apenas um conjunto de requisitos. Após essa etapa, os participantes construirão outro protótipo, considerando um conjunto de requisitos e as heurísticas de usabilidade para softwares científicos. Do mesmo modo, os participantes do segundo grupo realizarão as mesmas tarefas, mas em ordem invertida. Após a construção dos dois protótipos, os desenvolvedores opinarão a respeito do processo de desenvolvimento dos protótipos, de modo a verificar se a utilização das heurísticas foi benéfico ou não para o processo de desenvolvimento.

Após a avaliação empiríca dos desenvolvedores, ocorrerá a avaliação comparativa. Essa avaliação será dividida em duas partes. Na primeira parte, os protótipos desenvolvidos pelos participantes da avaliação empiríca dos desenvolvedores serão comparados, de modo a avaliar a qualidade da usabilidade dos dois protótipos e determinar qual grupo de protótipos apresenta a melhor qualidade na usabilidade. Os critérios da avaliação serão os benchmarks gerais de usabilidade presentes na literatura e o mecanismo de avaliação de usabilidade para softwares científicos criado no projeto. Por sua vez, na segunda parte, os protótipos construídos de softwares de bioninformática já existentes serão comparados com as suas respectivas versões originais, considerando os mesmos critérios da primeira parte da avaliação comparativa.

Por fim, ocorrerá a avaliação empírica dos usuários. Nessa etapa usuários de softwares de bioinformática serão divididos em dois grupos de estudo. Os participantes do primeiro grupo de estudo utilizarão a versão original dos softwares e em cada um deles terão que realizar tarefas pré-estabelecidas. Após isso, realizarão as mesmas tarefas, mas utilizarão os protótipos desenvolvidos. Do mesmo modo, os participantes do segundo grupo de estudo realizarão as mesmas tarefas, utilizando, dessa vez, primeiro o protótipo e depois o software original. Após a utilização dos softwares e protótipos os participantes opinarão a respeito da usabilidade presente em cada grupo (versão original e protótipo). Com essas três formas de avaliação, espera-se comprovar os benefícios proporcionados pelas heurísticas de usabilidade para softwares científicos.

V. Conclusão

Os softwares científicos são extremamente importantes para a realização das pesquisas científicas, uma vez que, auxiliam os pesquisadores a realizarem tarefas complexas. Por conta dessa característica desse tipo de software, o seu desenvolvimento é realizado, muitas vezes, pelos próprios pesquisadores, que detêm um grande conhecimento sobre o domínio da aplicação, mas não conhecem ou aplicam as boas práticas da engenharia de software. Consequentemente, os softwares

científicos apresentam uma baixa qualidade, principalmente nos quesitos de usabilidade.

A falta de usabilidade nos softwares científicos prejudica a divulgação e a utilização desses softwares por pesquisadores de áreas próximas. Assim, faz-se necessário o desenvolvimento de um mecanismo que busque auxiliar a presença de usabilidade nos softwares científicos.

Nesse sentido, entendemos que o desenvolvimento de heurísticas de usabilidade específicas para softwares científicos, que levem em consideração suas características particulares, como o público alvo de tais softwares e o conhecimento e experiências dos desenvolvedores, podem contribuir para a qualidade final do software científico e, consequentemente, com sua divulgação e utilização por outros pesquisadores.

Por se tratar de um projeto em fase inicial, esta pesquisa encontra-se na etapa de identificação do perfil dos desenvolvedores de softwares científicos.

REFERÊNCIAS

[1] SOMMERVILLE, I. *Engenharia de software. Tradução Ivan Bosnic e Kalinka G. de O. Gonçalves; revisão técnica Kechi Hirama–*. [S.l.]: São Paulo: Pearson Prentice Hall, 2011. ISBN 9788579361081.

[2] BAXTER, S. M. et al. Scientific software development is not an oxymoron. *PLOS Computational Biology*, Public Library of Science, v. 2, n. 9, p. 1–4, 09 2006. Disponível em: <https://doi.org/10.1371/journal.pcbi.0020087>.

[3] SEGAL, J.; MORRIS, C. Developing scientific software. *IEEE Software*, v. 25, n. 4, p. 18–20, July 2008. ISSN 0740-7459.

[4] LIST, M.; EBERT, P.; ALBRECHT, F. Ten simple rules for developing usable software in computational biology. *PLOS Computational Biology*, Public Library of Science, v. 13, n. 1, p. 1–5, 01 2017. Disponível em: <https://doi.org/10.1371/journal.pcbi.1005265>.

[5] MACAULAY, C. et al. Usability and user-centered design in scientific software development. *IEEE Software*, v. 26, p. 96–102, 01 2009. ISSN 0740-7459. Disponível em: <doi.ieeecomputersociety.org/10.1109/MS.2009.27>.

[6] PRESSMAN, S. R. Engenharia de software: Uma abordagem profissional. 7ª. *Edição. Rio de Janeiro–RJ. Editora McGraw-Hill*, 2011.

[7] GOULD, J. D.; LEWIS, C. Designing for usability: Key principles and what designers think. *Commun. ACM*, ACM, New York, NY, USA, v. 28, n. 3, p. 300–311, mar. 1985. ISSN 0001-0782. Disponível em: <http://doi.acm.org/10.1145/3166.3170>.

[8] RADATZ, J.; GERACI, A.; KATKI, F. Ieee standard glossary of software engineering terminology. *IEEE Std*, v. 610121990, n. 121990, p. 3, 1990.

[9] STANDARDIZATION, I. O. for; COMMISSION, I. E. *Software Engineering–Product Quality: Quality model*. [S.l.]: ISO/IEC, 2001. v. 1.

[10] MADAN, A.; DUBEY, S. K. Usability evaluation methods: a literature review. *International Journal of Engineering Science and Technology*, Engg Journals Publications, v. 4, n. 2, 2012.

[11] JIMENEZ, C.; LOZADA, P.; ROSAS, P. Usability heuristics: A systematic review. In: *2016 IEEE 11th Colombian Computing Conference (CCC)*. [S.l.: s.n.], 2016. p. 1–8.

[12] NIELSEN, J.; MOLICH, R. Heuristic evaluation of user interfaces. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, 1990. (CHI '90), p. 249–256. ISBN 0-201-50932-6. Disponível em: <http://doi.acm.org/10.1145/97243.97281>.

[13] NIELSEN, J. *Heuristics for User Interface Design: Article by Jakob Nielsen, 1995*. [S.l.], 10.

[14] DOHERTY, G.; COYLE, D.; MATTHEWS, M. Design and evaluation guidelines for mental health technologies. *Interacting with computers*, OUP, v. 22, n. 4, p. 243–252, 2010.

[15] CHILANA, P. K.; PALMER, C. L.; KO, A. J. Comparing bioinformatics software development by computer scientists and biologists: An exploratory study. In: *Proceedings of the 2009 ICSE Workshop on Software Engineering for Computational Science and Engineering*. Washington, DC, USA: IEEE Computer Society, 2009. (SECSE '09), p. 72–79. ISBN 978-1-4244-3737-5. Disponível em: <http://dx.doi.org/10.1109/SECSE.2009.5069165>.

[16] CHEN, T. Y. et al. An innovative approach for testing bioinformatics programs using metamorphic testing. *BMC Bioinformatics*, v. 10, n. 1, p. 24, Jan 2009. ISSN 1471-2105. Disponível em: <https://doi.org/10.1186/1471-2105-10-24>.

[17] LETONDAL, C. Participatory programming: Developing programmable bioinformatics tools for end-users. In: _____. *End User Development*. Dordrecht: Springer Netherlands, 2006. p. 207–242. ISBN 978-1-4020-5386-3. Disponível em: <https://doi.org/10.1007/1-4020-5386-X_10>.

[18] UMARJI, M. et al. Software engineering education for bioinformatics. In: *2009 22nd Conference on Software Engineering Education and Training. CSEET 2009(CSEET)*. [s.n.], 2009. v. 00, p. 216–223. Disponível em: <doi.ieeecomputersociety.org/10.1109/CSEET.2009.44>.

A Study of Applicability of Lion Optimization Algorithm to Perform Multiple Sequence Alignment

AMORIM, A. R.*; SATO, L. M.*
*Department of Computer Engineering and Digital Systems
Polytechnic School of University of São Paulo
E-mail: {anderson.amorim,liria.sato}@usp.br

***Abstract*—The multiple sequence alignment (MSA) is one of the most important tasks in bioinformatics. Different heuristics may be used to solve MSA problems, as progressive alignment and genetic algorithms (GA). Nonetheless, these approaches have known problems, as the error propagation on progressive alignment and local optima on GA, which directly affects the quality of the obtained alignments, in terms of biological significance. Thus, in this work we analyze the possibility to model an approach to solve the MSA problem, based on a new heuristic called lion optimization algorithm (LOA). This approach combines local and global search, which we think that may smooth the mentioned problems and obtain alignments with greater biological significance.**

***Keywords*— Bioinformatics; Multiple Sequence Alignment; Lion Optimization Algorithm.**

***Classification*— Doctorate degree.**

***Category*— Beginner.**

I. Introduction

Since the volume of biological data starts to grow, the bioinformatics has become important to provide computational tools to assist biologists in their analysis [1]. Among the main tasks performed in bioinformatics, we can cite pattern recognition on biological sequences [2] and multiple sequence alignment [3].

The multiple sequence alignment is a rearrangement of nucleotide or amino acid bases on more than two biological sequences, through the insertion of gaps. The main goal is to obtain the maximum similarity between the sequences to be aligned, which is measured by an objective function.

This task plays an important role on bioinformatics, because it can be used to function and structure prediction of unknown proteins and phylogenetic tree reconstruction [3].

There are many approaches to solve MSA problems, based on different heuristics, as progressive alignment [4], simulated annealing [5], tabu search [6], genetic algorithm [7], among others.

The progressive alignment is a well-known approach to solve MSA problems, because it generally obtain good results in a feasible time. We can see this strategy implemented on well-known tools as Clustal [8], [4], MUSCLE [9], among others.

Basically, we can divide the progressive alignment in three phases [4]. The first one is the pairwise alignment of all sequences on the process, using dynamic programming algorithms, as Needleman-Wunsch [10] or Smith-Waterman [11]. In the second phase, we calculate the distance matrix of the sequences and construct the phylogenetic tree. Finally, on the third phase, the closest sequences on the phylogenetic tree are progressively aligned on a profile, which will represent the multiple sequence alignment at the end of the process.

Despite the progressive alignment is able to obtain good results, this approach has the disadvantage of error propagation. An align mistake made on the initial steps will be propagated to the whole alignment, resulting on noisy alignments, which directly affects the quality of the analysis [12]. This generally occurs with completely unaligned and unrelated sequences. Moreover, Boyce *et al.* stated that the order of the input sequences on the alignment directly affects the biological quality of the results [13].

The genetic algorithm, unlike the progressive alignment, generally adapts the results through its execution, which means that it can obtain good results, even with unaligned and unrelated sequences [12]. We can see the use of GA to solve MSA problems in recent works [14], [7], [15].

The GA heuristic is based on Darwin's evolution theory, where individuals of a population will be exposed to selection pressure, crossover and mutation processes, in a way that the most adapted individuals will survive through the generations. When applied to the MSA problem, each possible alignment is an individual, the mutation operators will provide changes on gap positions and the crossover operation will create new alignments from two selected alignments [12].

Nonetheless, as other heuristics used to solve MSA problems, the GA has disadvantages. Lee *et al.* showed that genetic algorithms can easily reach a local optima, which means that the algorithm, in some cases, cannot find the better alignment, in terms of biological significance [16]. Moreover, due to the iterative nature of the GA, the runtime of the method is higher than other heuristics, as progressive alignment [17].

Thus, we can see that search for strategies to solve MSA that combine good results and feasible execution time remains to an open research field in bioinformatics. Thus, in this paper, we analyze the possibility of adapting a new optimization approach, called lion optimization algorithm (LOA) [18], to solve the MSA problem. We guess this strategy could outperform other approaches because of its simultaneous global and local search characteristic, which was similarly adopted by Rubio-Largo *et al.* [17], producing good results.

This paper is organized as follows: in section II we better

describe the multiple sequence alignment problem, in section III we show the characteristics of LOA and its operators and finally, in section IV, we show our conclusions.

II. Multiple Sequence Alignment

As we previously mentioned, the MSA is the alignment of more than two sequences of amino acids or nucleotides. Rubio-Largo *et al.* define MSA as follows [17]:

Let us assume a set of sequences to be aligned $S : \{s_1, s_2, ..., s_n\}$. The alphabet of nucleotides on DNA sequences is given by $\sum_{DNA} = \{A, T, C, G\}$ and the alphabet of amino acids on protein sequences is given by $\sum_{protein} = \{A, C, D, E, F, G, H, I, K, L, M, N, P, Q, R, S, T, V, W, Y\}$. The MSA of the sequences from S generates a new sequence set $S' : \{s'_1, s'_2, ..., s'_n\}$, which is defined over the same alphabet $\sum_{DNA}$ or $\sum_{protein}$ plus the gap symbol (-).

In the MSA, we want to insert gaps in specific positions to make the length of the sequences become the same, as we can see in Fig. 1. Basically, it can be represented as a matrix, where the rows are the sequences from S' and the columns are the aligned symbols.

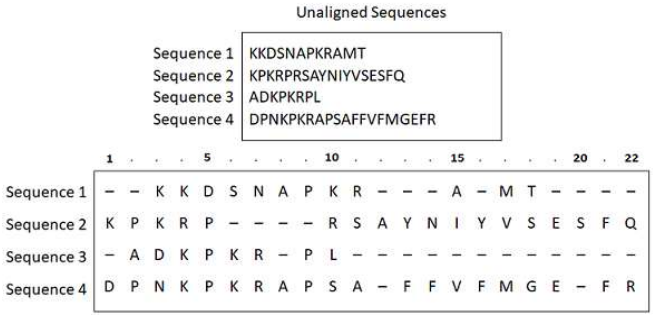


Fig. 1. An example of multiple sequence alignment.

The insertion of the gaps is given by some optimization approach, in order to search for the maximum level of correspondence of the aligned symbols. In other words, we want to maximize the number of columns whose aligned symbols are the same.

Thus, the lion optimization algorithm may be used as an optimization approach to solve the MSA problem. We claim that this approach would produce better results due to its characteristic of simultaneous local and global search, which will allow us performing a global alignment at the same time that we make some local adjustments on less similar regions.

In the next section, we will characterize LOA and give some insights of how we may adapt it to solve the MSA problem.

III. Lion Optimization Algorithm

The LOA is a metaheuristic proposed by Yazdani and Jolai [18], to solve numerical optimization problems, based on the group behavior of lions. The operators of this algorithm have global and local search characteristics, in order to simulate the behavior of lion and lionesses on tasks as hunting, reproducing, territory defending, among others. The authors stated that the simultaneous local and global search approach is an important fact that stood out LOA from other optimization algorithms.

Here, each possible solution is represented by a lion or a lioness. There are two main lion lifestyles: resident and nomads. The resident individuals organize themselves into groups, called prides. A pride has, generally, one or more male, five females and their cubs, which may be male or female. The nomad individuals, which may be male or female, will move sporadically on the territory. It is important to say that male and female lions mark their territory with urine. Thus, individuals may change their lifestyles at any time. Moreover, lionesses may migrate from one territory to another and change their lifestyle.

The lionesses of each pride hunt together, encircling the prey from different points. While the females go hunting, the male stay roaming and defending the territory. Moreover, a lion may mate with multiple lionesses, once they are in heat.

Nonetheless, LOA was initially proposed to solve numerical optimization problems. Thus, in this work we want to give an insight of how to adapt it to solve the MSA problem.

In our case, we can represent a possible alignment as a lion or a lioness. We may divide the individuals into their prides considering the fitness given by the objective function. Thus, for each pride, we would have a superior and an inferior threshold that represent the frontiers of the pride's territory. Thus, when a lion stay roaming its territory or lionesses go hunting, they may produce new alignments with new scores, which may change the thresholds, expanding their territory.

Thus, in the next subsections, we show the LOA operators issues and discuss how we could adapt them to MSA operators.

A. Hunting

In nature, lionesses go hunting in a group to provide food for their prides. The group has a collaboration instinct to encircle the prey. Thus, the group will be divided into three strategy positions: the left wing, the center and the right wing, as we can see in Fig. 2.

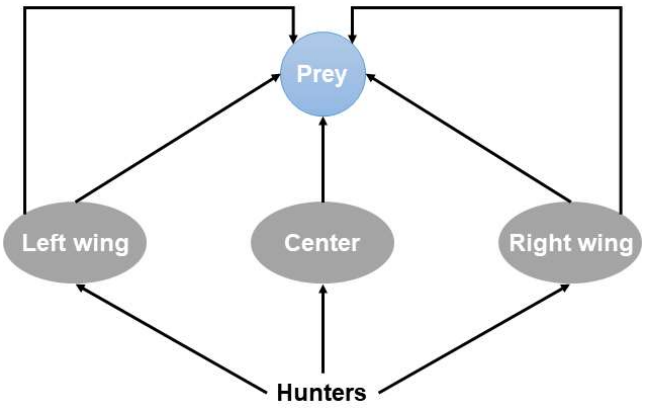


Fig. 2. The hunting strategy of female lions.

The lionesses are randomly selected and distributed among the hunting positions. Nonetheless, the strongest ones are directed to the center position and the other ones are randomly allocated among the left and right wings. Here, the strongest individuals means the individuals with greater fitness values, which is measured by some objective function. In our case, it would represent the better alignments.

To attack the prey, each lioness will be randomly selected from each attack position. The idea is to move the hunter to a new position, providing a new solution. If the new solution is better than the last one, the prey escapes and the hunter keep hunting until it does not improve its fitness value.

Moreover, if a prey escapes, the hunter will attack on the opposite position. Thus, if the attack came from the left wing, the hunter will now attack on the right wing position and vice-versa.

It is important to notice that the algorithm keeps the best visited position for each lioness. Thus, if an attack move degrades the quality of the solution, it will be ignored.

To adapt this operator to MSA, we can divide the alignment into three portions, which will represent the three attack positions, as we can see in Fig. 3. If the lioness is allocated to the left wing, we will provide some modifications on the first portion of the alignment. If the lioness is allocated to the center, we will provide some modifications on the second portion of the alignment. Finally, if the lioness is allocated to the right wing, we will provide some modifications on the third portion of the alignment.

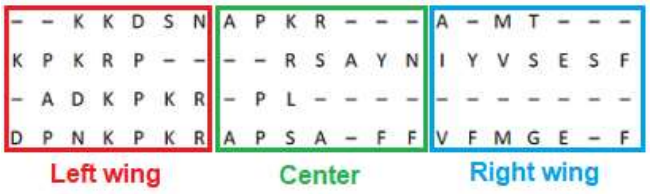


Fig. 3. The adapted hunting operator.

To provide modifications on the alignment portions, we can use the operators proposed by Rubio-Largo *et al.* [17]. These operators change the positions of gap blocks, extend or reduce their length, providing new alignments. The authors show that the effectiveness of the operators may lead to produce good results.

B. Roaming

While the females go hunting, the resident male lion roams its territory. When it is roaming, if the new position is better than the current one, the best solution is updated. This operator is an important local search strategy.

Thus, to adapt this operator to MSA, we may use local alignment strategies. It is worth to search for regions of less similarity on the alignment, caused by great occurrence of gap positions. This regions may degrade the overall quality of the alignment. Then, we could use a fast strategy, as progressive alignment, to realign the select region. Rubio-Largo *et al.* implemented a similar strategy using the *Kalign* [19] tool and reach good results [17].

In a similar way, nomads lions, male or female, move randomly in search space. This strategy avoid local optima solutions. To simulate this strategy, we could randomly insert or remove gap positions, which may generate new considered solutions.

C. Mating

An important way to exchange genetic information among the pride's member is mating. In a pride, the male lion mate with several lionesses, which are randomly select to produce offspring. It is basically a crossover operator, as we can see in genetic algorithms [12].

Thus, we could adapt this operator to MSA by randomly selecting the individuals to mate. Thus, we must define a cut point to recombination, which can be defined in the middle of the alignment, since the genetic information comes equally from the parents. Thus, new individuals will be generated combining the parts of each parent. Another strategy may be define the cut point randomly, as we can see in Gondro and Kinghorn work [12].

The mating operator will generate two new individuals, which will be considered cubs. On LOA, one of these new individuals will be set as male and the other one as female.

D. Defense

In nature, mature male lions defend their territory against nomads lions or cubs that reach sexual maturity. Thus, in combat, the defeated lion is driven out the pride and change its lifestyle, becoming nomad.

This way, we have basically two types of territory defending:

1) Against new mature resident males;
2) Against nomad males.

We can adapt this operator to the MSA problem using the thresholds that represent the frontiers of the prides and the fitness values of each lion. Considering the first option of battle, which cubs become mature residents, we may compare their fitness values with the value of the main resident lion. Thus, the lion with the least fitness value is driven out the pride and become nomad. In a similar way, in a fight of a resident lion against a nomad one, the nomad lion will become the resident male of the pride if it has a fitness value greater than the resident one, which will become a nomad.

E. Migration

Lionesses may have a migratory behavior, traveling from one pride to another or changing their lifestyle. This way, some lionesses are randomly selected from different prides and become nomads. Then, the old female nomads are randomly selected to fill the empty places on the prides. This operator is important to keep the population diversity.

The adaptation of this operator to work on MSA is more direct, since we can randomly select female individuals from different prides and simply change their lifestyles. Moreover,

we can order the old female nomads by their fitness values and fill the empty places of the prides with the individuals with greater fitness.

It is important to notice that the population equilibrium must be maintained. In each iteration, the lions with least fitness values will be replaced by the new ones with greater fitness values. The number of live lions must respect the user-defined parameter of the algorithm.

IV. Conclusion

Different heuristics can be used to solve multiple sequence alignments. Nonetheless, these heuristics have known problems, as error propagation on progressive alignment and local optima on genetic algorithms. Thus, proposing new strategies to perform MSA is a research field on bioinformatics.

In this work, we presented an insight of how lion optimization algorithm can be adapted to perform MSA. We guess that using LOA to solve MSA problems may lead to better results, with greater biological significance. This can be justified by the nature of the algorithm, which combines global and local search.

Thus, we can conclude that it is possible to use LOA to perform multiple sequence alignment. This heuristic may smooth the mentioned problems, since it can adapt its solutions, smoothing the error propagation problem, and its operators have strategies to escape local optima. Moreover, once the operators have no dependencies, we may execute different processes at the same time, using some parallel programming approach, as multithreading.

References

[1] KHURI, S. A bioinformatics track in computer science. In: ACM. *ACM SIGCSE Bulletin*. [S.l.], 2008. v. 40, n. 1, p. 508–512.

[2] KHAN, S. A.; HE, D.; VALVERDE, J. C. Pattern recognition in bioinformatics. *BioMed research international*, Hindawi Publishing Corporation, v. 2016, 2016.

[3] BAWONO, P. et al. Multiple sequence alignment. *Bioinformatics: Volume I: Data, Sequence Analysis, and Evolution*, Springer, p. 167–189, 2017.

[4] SIEVERS, F.; HIGGINS, D. G. Clustal omega for making accurate alignments of many protein sequences. *Protein Science*, Wiley Online Library, 2017.

[5] CORREA, J. M. et al. Parallel simulated annealing for fragment based sequence alignment. In: IEEE. *Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012 IEEE 26th International*. [S.l.], 2012. p. 641–648.

[6] LAMICHE, C.; MOUSSAOUI, A. An adaptive tabu search algorithm for obtaining alignment of multiple sequences. *Baltic Journal of Modern Computing*, University of Latvia, v. 2, n. 2, p. 75, 2014.

[7] KAYA, M.; KAYA, B.; ALHAJJ, R. A novel multi-objective genetic algorithm for multiple sequence alignment. *International Journal of Data Mining and Bioinformatics*, Inderscience Publishers (IEL), v. 14, n. 2, p. 139–158, 2016.

[8] THOMPSON, J. D.; HIGGINS, D. G.; GIBSON, T. J. Clustal w: improving the sensitivity of progressive multiple sequence alignment through sequence weighting, position-specific gap penalties and weight matrix choice. *Nucleic acids research*, Oxford university press, v. 22, n. 22, p. 4673–4680, 1994.

[9] EDGAR, R. C. Muscle: multiple sequence alignment with high accuracy and high throughput. *Nucleic acids research*, Oxford University Press, v. 32, n. 5, p. 1792–1797, 2004.

[10] NEEDLEMAN, S. B.; WUNSCH, C. D. A general method applicable to the search for similarities in the amino acid sequence of two proteins. *Journal of molecular biology*, Elsevier, v. 48, n. 3, p. 443–453, 1970.

[11] SMITH, T. F.; WATERMAN, M. S. Identification of common molecular subsequences. *Journal of molecular biology*, Elsevier, v. 147, n. 1, p. 195–197, 1981.

[12] GONDRO, C.; KINGHORN, B. A simple genetic algorithm for multiple sequence alignment. *Genetics and Molecular Research*, v. 6, n. 4, p. 964–982, 2007.

[13] BOYCE, K.; SIEVERS, F.; HIGGINS, D. G. Instability in progressive multiple sequence alignment algorithms. *Algorithms for molecular biology*, BioMed Central, v. 10, n. 1, p. 26, 2015.

[14] AMORIM, A. R. et al. An approach for coffee objective function to global dna multiple sequence alignment. *Computational biology and chemistry*, Elsevier, v. 75, p. 39–44, 2018.

[15] ORTUÑO, F. M. et al. Optimizing multiple sequence alignments using a genetic algorithm based on three objectives: structural information, non-gaps percentage and totally conserved columns. *Bioinformatics*, Oxford University Press, v. 29, n. 17, p. 2112–2121, 2013.

[16] LEE, Z.-J. et al. Genetic algorithm with ant colony optimization (ga-aco) for multiple sequence alignment. *Applied Soft Computing*, Elsevier, v. 8, n. 1, p. 55–78, 2008.

[17] RUBIO-LARGO, Á.; VEGA-RODRÍGUEZ, M. A.; GONZÁLEZ-ÁLVAREZ, D. L. Hybrid multiobjective artificial bee colony for multiple sequence alignment. *Applied Soft Computing*, Elsevier, v. 41, p. 157–168, 2016.

[18] YAZDANI, M.; JOLAI, F. Lion optimization algorithm (loa): a nature-inspired metaheuristic algorithm. *Journal of computational design and engineering*, Elsevier, v. 3, n. 1, p. 24–36, 2016.

[19] LASSMANN, T.; SONNHAMMER, E. L. Kalign–an accurate and fast multiple sequence alignment algorithm. *BMC bioinformatics*, BioMed Central, v. 6, n. 1, p. 298, 2005.

Big Data Quality Issues Identified on Data Life Cycle

Questões de Qualidade de Dados em Big Data Identificadas no Ciclo de Vida dos Dados

FRANCISCO, M.M. C.; SOUZA, S. N.A.; ALMEIDA, J.R.
Escola Politécnica da Universidade de São Paulo
maritza@vantageinfotech.com.br, ssouza@usp.br, jorgerady@usp.br

***Abstract*—Currently, one of the greatest competitive advantages for modern organizations is the ability to generate knowledge and innovation from the analysis of the vast volume of data available, inside and outside organizations. Numerous companies have created new business models, improved the quality of their services, optimized processes and reduced operational costs through the effective use of data not only from their internal systems, but also from social networks, IoT (Internet of Things) for example. Data quality (QD) is a crucial issue in this scenario, which becomes more complex, requiring, among other requirements, the handling of unstructured data, at an increasing rate. This article identifies issues related to data quality in the big data throughout the data life cycle, representing an initial study of the doctoral research whose objective is the proposition of a reference architecture for big data quality.**

***Keywords*— data quality; big data quality; data life cycle.**
Classification*—*Doctorate degree.
Category*— *Beginner.

Resumo— ***Atualmente, uma das maiores vantagens competitivas para as organizações modernas é a capacidade de gerar conhecimento e inovação a partir da análise da imensa volumetria de dados disponível, dentro e fora das organizações. Inúmeras empresas têm criado novos modelos de negócio, melhorado a qualidade de seus serviços, otimizado processos e reduzido custos operacionais por meio do uso efetivo dos dados oriundos não somente de seus sistemas internos, como também das redes sociais, IoT (internet of things), por exemplo. A qualidade dos dados (QD) é uma questão crucial neste cenário, que se torna mais complexa, por exigir, dentre outros requisitos, o tratamento de dados não estruturados, em uma velocidade cada vez maior. Este artigo identifica questões relacionadas à qualidade dos dados em big data ao longo do ciclo de vida dos dados, representando um estudo inicial da pesquisa de doutorado cujo objetivo é a proposição de uma arquitetura de referência para QD em big data.***

***Palavras-chave*— qualidade de dados; qualidade de dados em big data; ciclo de vida dos dados.**
Classificação*— *Doutorado.
Categoria*— *Iniciante.

I. INTRODUÇÃO

A era dos dados, caracterizada pela abundância de dados gerados, processados e consumidos em altíssima velocidade, advindos de fontes e formatos variados, aumenta a complexidade dos problemas de qualidade de dados dos ambientes analíticos modernos, notadamente baseados em big data [1].

O tratamento da qualidade de dados tem sido abordado em diversas pesquisas, [1] e [2]. Uma vasta gama de dimensões de QD, metodologias e técnicas para medição, avaliação e gerenciamento da QD foram propostas. Todavia, as características do ambiente de big data trazem a necessidade de se adaptar ou estender essas propostas. O tratamento de dados não estruturados, a velocidade na identificação e correção de erros nos dados de modo a garantir a oportunidade de uso, são exemplos de requisitos para a adaptação das abordagens existentes.

O objetivo da pesquisa de doutorado, da qual este artigo faz parte, é propor uma arquitetura de referência para QD em big data. Uma arquitetura de referência mostra quais funcionalidades são geralmente necessárias em um determinado domínio ou para a resolução de uma determinada classe de problemas. Ela evidencia como estas funcionalidades são divididas e como a informação flui entre as suas partes, [3]. A identificação das funcionalidades que farão parte da arquitetura a ser definida, considerará os requisitos de qualidade de dados em big data identificados por meio dos problemas, questões e desafios pesquisados na literatura.

O ciclo de vida dos dados analíticos foi escolhido para ser o foco da identificação inicial de questões e desafios de QD em big data, por englobar um conjunto de processos que transformam dados em informação e informação em conhecimento [4]. A qualidade de dados deve ser observada como um processo a ser executado durante as fases deste ciclo de vida, evidenciando possíveis funcionalidades que a arquitetura de referência deverá suportar. Desta forma, a questão de pesquisa que orientou este artigo foi:

- Considerando o ciclo de vida de dados analíticos em big data, quais questões e desafios de qualidade de dados devem ser observadas em cada fase deste ciclo?

Esta pesquisa apresenta um ciclo de vida unificado de dados, baseado em propostas já existentes e compila, sem esgotar o assunto, as questões de QD observadas em cada fase deste ciclo unificado.

Este artigo está estruturado em 5 seções. A seção 2 apresenta os estudos relacionados ao tema. Na seção 3 são apresentados os desafios e problemas gerais de QD em big data evidenciados na literatura. A seção 4 identifica as questões e problemas de QD no decorrer do ciclo de vida unificado dos dados. A seção 5 conclui o artigo e propõe trabalho futuros.

II. TRABALHOS RELACIONADOS

As referências [5] e [6] fornecem uma descrição sistemática e comparativa de questões de pesquisa relacionadas à qualidade de dados e informações. Em relação a big data, evidenciam a importância dos conceitos confiabilidade e proveniência.

Ciclo de vida dos dados é definido em [4], como o conjunto de processos que transforma dados brutos em conhecimento. [1] apresenta um ciclo de vida composto por 5 fases: (1) aquisição / registro de dados, responsável pela coleta e gravação dos dados, além da catalogação dos metadados; (2) extração e limpeza cujo objetivo é preparar e transformar o dado para a análise; (3) integração responsável pela consolidação e unificação de conceitos oriundos de bases heterogêneas; (4) análise e modelagem que constroem modelos que solucionam problemas de negócio; (5) a interpretação e a visualização que tornam os dados mais compreensíveis, permitindo o rastreamento das premissas e análises feitas.

[7] e [8] apresentam o ciclo de vida dos dados composto por 5 etapas: coleta, preparação, análise, visualização e acesso. Na coleta os dados são extraídos ou recebidos do provedor de dados. A preparação trata os dados para que as análises sejam realizadas. Na etapa de analise, implementam-se as técnicas para extrair conhecimento da base de dados. A visualização prepara os resultados da etapa de análise para serem apresentados ao consumidor de dados, de modo a comunicar, da melhor forma, o significado e o conhecimento dos dados. O acesso é resultado das solicitações do consumidor para visualizar os dados analisados.

[9] apresenta a extração, carga e pré-processamento, processamento, análise, carga e transformação, interface e visualização como processos para a produção dos dados.

O ciclo de vida proposto por [7] e [8] centram-se na produção do dado analítico, considerando que os dados já estão presentes no ambiente big data. As atividades deste ciclo são suportadas pela camada *Big Data Application Provider* da arquitetura de referência proposta nestas referências. A coleta dos dados a partir das diversas origens é uma atividade realizada na camada *Data Provider* da arquitetura de referência, não fazendo parte do conceito de ciclo de vida dos dados. As propostas [1] e [9] fazem menção ao ciclo completo, desde as origens, até o efetivo consumo dos dados.

Este artigo propõe um ciclo de vida unificado que representa a junção dos conceitos propostos em [1], [8] e [9], detalhados na sessão IV.

III. BIG DATA QUALITY – DESAFIOS E PROBLEMAS GERAIS DE QD

Além dos problemas de qualidade de dados presentes nos ambientes tradicionais, tais como, dados faltantes, dados duplicados, dados inconsistentes, imprecisos, dentre outros, alguns problemas se agravam ou novos surgem no contexto de big data decorrentes, por exemplo, de dados *streaming*, análise de dados em tempo real, preponderância de dados não estruturados, [10]**.** [5] e [6] afirmam que pesquisar e usar as informações armazenadas em bilhões de páginas da Web representam desafios significativos, porque essas informações e respectiva semântica são geralmente mais complexas e dinâmicas do que no ambiente tradicional. Os dados da Web são altamente diversificados, e combinam vários tipos de mídia e dados. Dois paradigmas tornam-se indispensáveis para caracterizar a qualidade dos dados da Web: a confiabilidade e a relevância. A confiabilidade é caracterizada por meio da credibilidade e reputação das fontes de dados, bem como da verificabilidade. A proveniência é um conceito considerado complexo e que remete a todos os caminhos percorridos pelo dado até ser inserido no ambiente de big data, o que inclui o entendimento sobre quais dados foram captados, com quais regras e a motivação que levou a sua coleta.

Além das questões relacionadas à QD em dados da Web, [5] enfatiza a influência dos tipos de fontes de dados na complexidade da qualidade de dados em big data. As fontes de informação de origem humana incluem dados de redes sociais, emails, blogs, comentários, pesquisas em mecanismos de busca, videos, dentre outros. As fontes de dados mediadas por processos podem consistir em dados produzidos por órgãos instituições públicos e dados produzidos pelo setor privado (transações comerciais, registros bancários / de ações, comércio eletrônico, cartões de crédito, etc.). As fontes de dados gerados por máquinas incluem sensores fixos, sensores móveis, vídeos, imagens de segurança, arquivos de log. Falhas nos processos de mediação ou mesmo no funcionamento da máquina podem produzir dados com baixa qualidade, por exemplo, dados incompletos, errados, imprecisos.

Durante a tarefa de processamento de dados *streaming*, os erros inerentes aos sensores podem ser amplificados. Além disso, novos erros podem ser introduzidos por meio de leituras perdidas, leituras não confiáveis e variação nos erros devido ao meio ambiente.

Os desafios de QD considerados como principais em [2] são: (a) a diversidade de fontes de dados, que traz uma grande variedade de tipos de dados e estruturas de dados complexa, aumentando a dificuldade de integração desses dados; (b) o grande volume de dados, que aumenta a dificuldade para se avaliar a qualidade dos dados dentro de um período de tempo razoável e (c) a volatilidade dos dados reduzindo a oportunidade de uso dos dados.

IV. QUALIDADE DE DADOS AO LONGO DO CICLO DE VIDA DO DADOS

No ciclo de vida do dado em big data, cada estágio de transformação ou processamento dos dados pode alterar o seu conteúdo e a forma de representa-los, [11]. Este contexto aumenta a importância de se estabelecer uma correta ligação entre os dados de origem e os dados processados, mantendo a integridade de referência. Isso enfatiza os conceitos como dinamicidade/variabilidade ou integridade de ligação ou referência e proveniência. Dinamicidade, ou variabilidade, reflete a constante mudança dos dados, que são comumente classificados como dados em movimento, dados em repouso

ou dados em processamento. A possibilidade de se reutilizar e redirecionar os conjuntos de dados iniciais para novas análises de dados também traz desafios relacionados à integridade de referência e à proveniência dos dados. Além disso, a agregação de dados pode envolver dados de diferentes domínios e semanticamente diferentes.

Este artigo baseia-se no ciclo de vida unificado que representa a junção dos conceitos propostos em [1], [8], [9], conforme o Fig. 1. A unificação deste ciclo foi realizada seguindo os seguintes passos: (1) Análise de cada atividade apresentada nos ciclos de vida propostos; (2) Eliminação das atividades duplicadas; (3) Unificação das atividades restantes.

A seguir, cada fase é apresentada considerando suas atividades e questões de QD relacionadas.

Figura 1: Ciclo de Vida Unificado de Dados

A. Coleta

A fase de Coleta do ciclo de vida unificado agrupa as seguintes atividades: (a) Extração a partir de diversas origens; (b) Carga em um repositório de dados brutos; (c) Retirada ou mascaramento de dados confidencias; (d) Registro dos metados relacionados à proveniência.

Dados incorretos ou imprecisos podem ser coletados de sensores quebrados ou devido a limitações nos dispositivos de medição. Aplicativos não testados podem produzir dados com falha, caso em que problemas de qualidade são causados por erros no código. Dados desatualizados, conflitantes, intencionais ou acidentalmente errados ou enganosos (por exemplo, spam) podem ser coletados de blogs, notícias e mídias sociais.

Ao se extrair os dados das diversas fontes, muitos dados podem não ser de interesse, e deveriam ser filtrados. Por exemplo, a maioria dos dados gerados pelas redes de sensores é altamente redundante, o que poderia ser filtrado, [12]. Um desafio é definir esses filtros de forma que eles não descartem informações úteis.

Alguns conjuntos de dados contêm elementos de dados confidenciais, [7] e [8]. Seja por conformidade regulatória ou por nível de sensibilidade, tais elementos de dados podem ser alterados (mascarados) ou removidos. Informações pessoalmente identificáveis (PII), é um exemplo deste tipo de elemento de dados. Assim a segurança e

É importante que as interfaces de captura de dados forneçam os recursos para se registrar informações acerca do provedor de dados, dos mecanismos de identificação dos dados de interesse, os tipos de acessos utilizados, que devem estar compatíveis com os acessos permitidos, os requisitos de segurança de dados e de privacidade, dentre outras informações. Portanto, as interfaces deveriam fornecer os meios para o devido registro dos metados, especialmente aqueles relacionados à proveniência. Por exemplo, em experimentos científicos, detalhes em relação a condições e procedimentos específicos podem ser necessários para que os resultados possam ser interpretados corretamente, e é importante que esses metadados sejam registrados com dados observacionais no momento de sua captura.

Do ponto de vista de metadados, ressalta-se a importância da (1) completude, (2) clareza dos dados registrados e (3) disponibilidade dos metadados para os diversos tipos de usuários ou processos subsequentes.

B. ETL

Após a conclusão da coleta de dados brutos, os dados serão transferidos para uma infraestrutura de armazenamento de dados para processamento e análise, [12]. A fase de ETL do ciclo de vida unificado agrupa as seguintes atividadades: (a) extração dos dados a partir do repositório de dados brutos; (b) preparação dos dados, que pode englobar tarefas como validação, limpeza, remoção de outliers, conversões, padronizações, reformatações, agregações, derivações, particionamento, preparação para o armazenamento, visualização); (c) integração de dados; (d) carga dos dados nas bases destino; (e) registro de metados.

Em ambientes distribuídos, há vários tipos de heterogeneidades, que podem ser observadas tanto em termos de tecnologia (diferentes Sistemas Gerenciadores de Banco de Dados), quanto de esquema (representações distintas) ou em termos de instância (valores conflitantes), [3]. Neste cenário, a integração ganha relevância, tendo como principal meta permitir que um usuário acesse os dados por meio de uma representação consistente que permita uma visão unificada desses dados. [12] afirma que uma representação de dados inadequada reduzirá o valor dos dados originais, podendo impedir a análise de dados efetiva.

As grandes preocupações desta fase relacionam-se à qualidade intrínseca do dado, à qualidade representacional e à proveniência. A qualidade intrínseca relaciona-se ao conteúdo do dado em si, a qualidade representacional enfatiza a consistência de representação do dados em todos os ambientes em que este dado aparecer e à proveniência explicita todo o processamento que foi realizado , [13].

Observa-se inúmeras questões a serem tratadas nesta fase, das quais destacam-se: (1) a integração adequada de dados; (2) garantia da derivação correta de esquemas das diversas bases que podem compor o ambiente. Por exemplo, a correta derivação do modelo dimensional (adequado para ambiente de *data warehouse*) a partir do modelo relacional (comumente utilizado para ambientes transacionais); (3) a identificação de nomes iguais para conceitos distintos, e de nomes distintos para o mesmo conceito; (4) padronização, limpeza, enriquecimento de dados, tratamento de duplicidades, redundâncias, inconsistências; (5) tratamento de dados não estruturados; (6) garantia do registro dos metadados,

especialmente daqueles relacionados à proveniência; (7) garantia da rastreabilidade de todo o processo realizado.

C. Análise

A fase de Análise do ciclo de vida unificado agrupa as seguintes atividadades: (a) transformar um problema de negócio em um problema de dados; (b) modelar uma solução; (c) analisar os dados resultantes da execução do modelo; (d) carga em bases analíticas para exploração.

A fase de análise é altamente dependente do contexto e do uso que se pretende fazer do dado, [5]. Com a introdução de novos paradigmas de armazenamento, que incluem dados não estruturados, as técnicas de análise devem ser modificadas para diferentes tipos de dados.

Algumas questões de QD relevantes desta fase são: (1) entendimento adequado do problema e a escolha adequada do modelo analítico a ser construído, de tal forma que seja possível a geração de resultados significativos. Tudo começa na formulação adequada das questões de análise; (2) preparação dos dados de acordo com o modelo/algoritmo que se deseja aplicar; (3) atualidade adequada dos dados; (4) análise em tempo hábil; (5) garantia da quantidade, nível de detalhe e de histórico de dados suficientes pata a execução das análises; (6) garantia de acesso seguro, privado e adequado; (7) garantia da disponibilidade de metadados; (8) para a execução de algumas análises, bases de dados específicas são criadas, como, por exemplo, *data marts*. A aplicação incorreta da técnica de modelagem, bem como a derivação/agregação inadequada de conceitos, pode disponibilizar dados incorretos e incoerentes para as análises.

D. Visualização

A fase de Visualização do ciclo de vida unificado agrupa as seguintes atividades: (a) visualização e interpretação os dados e (b) registro dos metadados que indicará todo o caminho de análise realizado e as interpretações e conclusões alcançadas.

Questões de QD importantes na fase de visualização: (1) visualização adequada ao tipo de análise e ao tipo de público para não dificultar a manipulação, interpretação e uso dos dados; (2) garantia do acesso, com a devida segurança e privacidade; (3) proveniência, disponibilizando todas as hipóteses feitas, o rastreamento das análises, informações sobre como cada resultado foi derivado a partir de quais dados de entrada.

V. Conclusão

Os problemas e questões de qualidade de dados presentes nos ambientes tradicionais podem ser observados também no ambiente de big data, porém, alguns problemas se agravam ou novos surgem neste contexto devido a variedade de dados e a velocidade com a qual os dados são produzidos, processados e consumidos. No estudo realizado, foi verificada a grande importância das questões relativas à reputação das fontes, completude, relevância, confiabilidade dos dados, atualidade e representação que estão intimamente relacionadas à veracidade (confiabilidade e credibilidade dos dados) e ao valor (relevância) dos dados, conceitos que ajudam a definir o que é big data. As questões relacionadas à segurança e proveniência ganha um papel crucial em praticamente todas as fases do ciclo de vida dos dados, pois cada estágio pode alterar o seu conteúdo e a forma de representa-los.

Como questões futuras de pesquisa podem ser citadas: (a) quais dimensões de QD podem ser examinadas em cada fase do ciclo de vida do dado?; (b) quais tecnologias podem ser utilizadas para a solução das questões de QD identificadas neste trabalho? (c) como garantir o registro e a disponibilidade da proveniência dos dados? (d) revisão sistemática sobre os problemas de QD em Big data.

References

[1] M. Toivonen, “Big Data Quality Challenges in the Context of Business Analytics,” *2015 Int. Conf. Comput. Commun. Secur.*, pp. 1–9, 2015.

[2] L. Cai and Y. Zhu, “The Challenges of Data Quality and Data Quality Assessment in the Big Data Era,” *Data Sci. J.*, vol. 14, no. 0, p. 2, 2015.

[3] M. Maier, “Towards a Big Data Reference Architecture,” no. October, pp. 1–144, 2013.

[4] NIST Big Data Public Working Group, “NIST Special Publication 1500-1 - NIST Big Data Interoperability Framework: Volume 1, Definitions,” *NIST Spec. Publ.*, vol. 1, p. 32, 2015.

[5] C. Batini and M. Scannapieco, *Data and Information Quality*. 2016.

[6] C. Batini, A. Rula, M. Scannapieco, and G. Viscusi, “From Data Quality to Big Data Quality,” *J. Database Manag.*, vol. 26, no. 1, pp. 60–82, 2015.

[7] T. Subgroup, “NIST Special Publication 1500-2 NIST Big Data Interoperability Framework : Volume 2 , Big Data Taxonomies DRAFT NIST Big Data Interoperability Framework : Volume 2 , Big Data Taxonomies,” vol. 2, 2015.

[8] N. B. D. P. W. G. (NBD-PWG), “NIST Special Publication 1500-6 : NIST Big Data Interoperability Framework - Reference Architecture,” vol. 6, pp. 1–62, 2015.

[9] P. Pääkkönen and D. Pakkala, “Reference Architecture and Classification of Technologies, Products and Services for Big Data Systems,” *Big Data Res.*, vol. 2, no. 4, pp. 166–186, 2015.

[10] D. Rao, V. N. Gudivada, and V. V Raghavan, “Data Quality Issues in Big Data.”

[11] Y. Demchenko, C. De Laat, and P. Membrey, “Defining architecture components of the Big Data Ecosystem,” *2014 Int. Conf. Collab. Technol. Syst. CTS 2014*, no. May, pp. 104–112, 2014.

[12] M. Chen, S. Mao, and Y. Liu, “Big data: A survey,” *Mob. Networks Appl.*, vol. 19, no. 2, pp. 171–209, 2014.

[13] D. M. Strong, Y. W. Lee, and R. Y. Wang, “Data Quality in Context. Communication of the ACM,” vol. 40, no. 5, pp. 103–110, 1997.

Cooperative Intrusion Detection System for Software-Defined Wireless Sensor Networks

NUNEZ, G. A.; MARGI, C. B.
E-mail: {gustavoalonso.nunez,cintia}@usp.br

***Abstract*—Software-defined networking (SDN) is a paradigm that has been proposed as a solution for current wireless sensor networks (WSN) challenges. One of the main challenges of WSN is security. Even though SDN can solve some of WSN security issues, its characteristics open new vulnerabilities. In this work we propose CID-SDN, a first approach to a cooperative Intrusion Detection System (IDS) for SDWSN. This IDS aims to detect denial of service attacks meant to exhaust the SDN controller resources and to saturate the nodes flow table. We propose a cooperative approach with two mechanisms: one using sensor nodes to help the controller in the detection and the other one using multiple controllers. Finally, we propose to compare the distributed approach performance with a centralized IDS approach.**

***Keywords*— Software-defined networking; Wireless sensor networks; software-defined wireless sensor networks.**

***Classification*— doctorate degree.**

***Category*— Beginner**

I. Introduction

Wireless sensor networks (WSN) are formed by devices with several constraints, such as: low processing power, low storage capacity, limited bandwidth, and limited energy. This inherent resource-constrained characteristic has motivated the research of novel solutions to face WSN's current challenges. Software-defined networking (SDN) is one of those paradigms that several authors proposed as a real solution [1].

SDN is a paradigm to manage networks that aims to extend the network programability [2]. SDN decouples the control plane from the data plane. The control logic resides in a logically centralized controller and the network devices become simple forwarding devices [3]. The implementation of SDN into a WSN is commonly known as software-defined wireless sensor networks (SDWSN) and there are proposals in the literature [1][4].

One of the main challenges faced by WSN is security. WSN have certain resources and deployment characteristics that differentiate them from wired and non-resource-constrained networks, what makes them more vulnerable to security attacks [5]. For example, processing power constraints hampers the implementation of robust mechanism systems. Also, the open environments deployments increment the risk of physical attacks.

SDN has characteristics that can bring benefits to the network security, including WSN [6]. The global view that the SDN controller has can be used to implement network-wide intrusion detection system (IDS) or to detect a malicious switch behavior. Also, SDN can react to countermeasure an intrusion attack using conditional rules to change how a switch has to respond in certain conditions or with certain type of packets. On the other hand, the SDN architecture is exposed to new security threats. The control plane is vulnerable to denial of service attacks (DoS). If multiple hosts flood the network with packets the switches do not know how to manage, it could generate a huge amount of queries to the controller, utilizing its processing power and causing the queries to be delayed or dropped. Also, there can be attacks that compromise the controller and thus the intruder takes control of the network. In this case, the intruder can compromise the whole network by changing the rules of all the nodes.

SDN can bring benefits to WSN in terms of security [1]. The controller's global view and the information it could obtain about the network are special characteristics that can be used to implement IDSs that were unfeasible in traditional WSN [1][7]. Also, Pritchard *et.al.* [8] state that SDN relieves sensor nodes resources that can be used to implement more complex cryptography methods than used in traditional WSN. Conversely, SDN introduces new vulnerabilities to WSN. An attack to the SDN controller can compromise the entire network. Thus, robust mechanisms to secure the SDN controller are also a challenge.

The objective of this work is to present a first approach to a cooperative IDS for SDWSN. We propose two mechanism. One mechanism using sensor nodes that analyze traffic and help the controller to detect an intrusion. The second mechanism uses multiple controllers, where each controller can detect an intrusion independently. Then, we propose to compare the cooperative IDS performance with a centralized IDS.

The remainder of this paper is organized as follows. Section II presents a security analysis of SDN and SDWSN. In Section III we explain the cooperative IDS and the centralized approach. Section IV presents the methods to carry out the implementation and performance comparison. Finally, Section V concludes the paper.

II. Security analysis

In this section we review the new threats that open the implementation of SDN. Then, we analyze those new threats in the context of SDWSN.

A. SDN security threats

As metioned in Section I, SDN can bring benefits for future networks but also it opens new security challenges. The

separation of the planes and the centralization of the control decisions turns the network prone to attacks that may not affect traditional networks. The analysis of those new threats can be divided in three groups [9]: application plane, control plane, and data plane. The interaction among those planes is depicted in Figure 1.

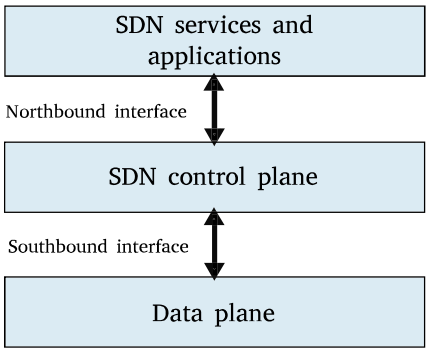


Fig. 1. SDN planes

The application plane is composed by a set of services and applications which are interfaced with the SDN controller. Malicious applications that are not detected or stoped early enough could harm the entire network [10]. Illegal access, from applications to the controller and security rules conflict are two main security threats for the application plane [11].

The data plane is conformed by the devices responsible to forward the packets. These devices are vulnerable to security attacks because they are a direct entry point to access the network [11]. Two of the attacks that surge with the SDN implementation are the modification and saturation of the flow tables. The flow table has the forwarding information established by the control plane. Modifications in the flow table will lead to a wrong treatment of the packets received and sent. Also, an intruder can attack a specific device sending packets without a flow rule defined. This will cause several requests of flow rules to the controller that could saturate the flow table with illegal flow rules.

The control plane is pointed out as the most attractive plane to be attacked [9][11] because it is reponsible for the overall management of the network [10]. This plane is prone to DoS attacks. An intruder may flood the network with flow rule requests, which could lead to an exhaustation of resources of the controller. This attack can be intensified using multiple and distributed intruders, which is known as distributed DoS (DDoS). SDN was originally designed as a single controller architecture, which in terms of security is an attractive characteristic for attackers. Distributed control solutions have been proposed to reduce the risk of one physical controller failure [12] [13], but these solutions have open new authorization, authentication and privacy issues [11].

B. SDWSN security analysis

The threats and vulnerabilities explained in Section II-A are also valid for SDWSN. Moreover, due to resources constraints, most of the security mechanisms designed for not resources constrained SDN networks have to be adapted or redesigned. This is one of the major challenges for SDWSN security. Assuming that there is the possibility to have an SDN controller without resources constraints, the forwarding devices and the interface between the SDN controller and the rest of the network are elements to focus security research in SDWSN.

One difference between SDWSN and the wired networks that use SDN is that the first one can not use out-of-band control, which means that the control traffic and data traffic are forwarded through the same link. In the case of a man-in-the-middle attack, the intruder can access both type of packets. If the man-in-the-middle attack is combined with another attack, such as a black hole attack, it could hamper both data and control plane [14].

In SDWSN the forwarding devices have low storage capacity, which limitates the memory assigned for flow tables and buffers. These constraints make the forwarding devices prone to saturation attacks. Also, SDWSN networks are characterized for having a limited bandwidth and low processing power. This means that a saturation attack can also result in a DoS attack.

As mentioned before, the controller needs a gateway to communicate with the network. This gateway has a radio module that may have no energy constraints but limited bandwidth. This issue turns the gateway into a bottleneck that, even thought the controller could have enough resources to overcome an attack, it can take the controller out of communication.

Ajaeiya *et.al.* [15] and Sangodoyin *et.al.* [16] proposed countermeasures for DoS attacks for non-restricted networks and using OpenFlow. Yuan *et.al.* [16] proposed a quality of service (QoS) aware mitigation strategy for flow tables overload also for non-restricted networks and using Openflow. Grigoryan *et.al.* [17] proposed a cooperative mechanism for IoT using SDN. Grigoryan *et.al.* proposal consider an heterogeneous network but using non-resources-constrained switches and controllers, and also using OpenFlow.

Previous works lack proposals for DoS attacks countermeasures in SDWSN, where most of devices are resource-constrained. Also, most of proposals are based on OpenFlow, which is not suited for SDWSN [1][20]. To fill this gap, we propose an IDS for DoS attacks that address the resource constraints issues in SDWSN and is not OpenFlow based.

III. Cooperative IDS for DoS attacks

In Section II-A we explained how a DoS attack works in an SDN network, and in Section II-B we explained its outcomes for SDWSN. In this section we proposed CID-SDN, a cooperative IDS solution for DoS attack in SDWSN. This solution aims to avoid the SDN controller's resources exhaustation and to avoid the forwarding devices' flow table saturation.

The IDSs can be briefly classified in two types: signature-based and anomaly-based [18]. The signature-based mechanisms is commonly used for known attacks or threats. The attack pattern is previously stored in the system to compare

it with captured events and detect a possible intrusion. Conversely, the anomaly-based mechanisms monitors the regular activities to detec deviations from the expected behavior.

We propose two mechanism for CID-SDN. In the first mechanism, named CID-SDN-1, there are defined two types of sensor nodes: low processing power (LPP) node and high processing power (HPP) node. The CID-SDN-1 main idea is to use the HPP nodes as a first traffic analyzer running a signature-based IDS. To detect the attack, we will analyze the traffic generated by flow rule request sent from all the sensor nodes to the controller. The controller will define an exclusive flow for this traffic including at least one HPP node in the route when it be feasible. When the HPP node detects an attack, it warns the controller about it and the controller decides how to react to countermeasure it. In the case the HPP was unable to detect the attack, the SDN controller will be running both signature-based and anomaly-based IDSs. Thus, it will work as an hybrid IDS but in a cooperative way. As depicted in Figure 2, even though the controller and the sink are located in the same node, the application data and the flow rule request use different routes. The controller takes this decision in order to include one HPP in the flow rule request before reaching the controller.

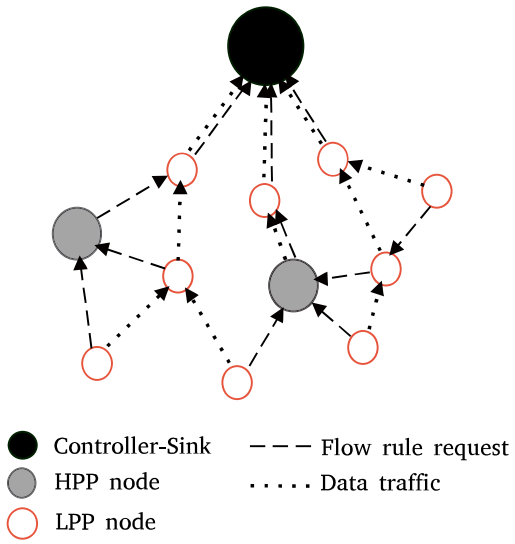


Fig. 2. Flow traffic using HPP and LPP nodes

In the second approach, named CID-SDN-2, we propose to use multiple SDN controllers. This approach brings scalability to the network. The controllers will have enough information to analyze the traffic and also they could react to countermeasure the attack. For this case will not be necessary to establish an exclusive flow for flow rules requests, the information will be shared with the closest SDN controller. On the other hand, it will be necessary to develop the Eastbound and Westbound interfaces to establish communication between controllers.

We will implement a third scenario using only one SDN controller and without HPP nodes. The sensor nodes will periodically share their traffic information with the SDN

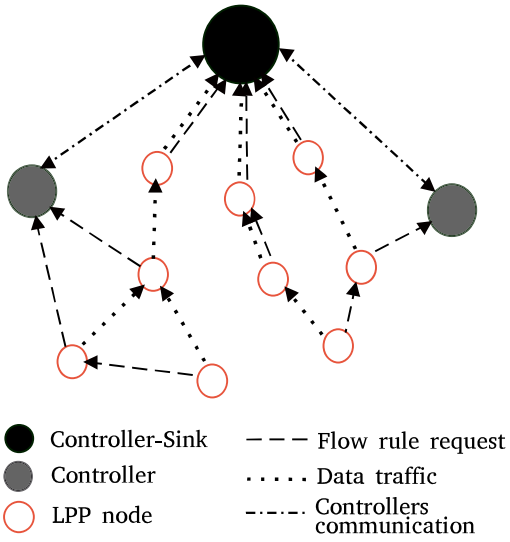


Fig. 3. Flow traffic using multiple controllers

controller. Both types of IDS will be running on the controller. This approach is commonly used in OpenFlow networks [15].

We belive that using CID-SDN-1 we will be able to detect DoS attacks before them affect the controller, avoiding the controller's resources exhaustation and a flow table saturation in the sensor nodes. Using CID-SDN-2 the flow rule request will be distributed, alleviating the overhead of each controller. This can bring more time to detect and countermeasure a DDoS attack if compared with the centralized approach.

IV. Methods

The implementation will be conducted using ContikiOS [19] and IT-SDN [20], a framework for SDWSN. IT-SDN's source code is totally open and its architecture is independent of the operating system. We will use COOJA for simulations and the three IDS mechanisms will be tested using real devices, such as TelosB and SensorTag, running in a testbed deployed in our laboratory.

We will implement the three mechanisms explained in Section III to compare their performances. The metrics to compare their performances are divided in: network performance metrics and security metrics. The network performance metrics are: delivery rate, total delay, packets overhead, and energy. The total delivery rate is calculated dividing the total number of packets sucessfully received by the total packets sent. The total delay is the average of the time the packets spent to reach the destination. The overhead is quantified as the total amount of packets per minute. The energy consumption is the average energy consumption per minute of all nodes, excluding the sink node and the controller node.

The security metrics are: classification rate (CR), detection rate (DR), false positive rate (FPR), and precision (PR). To calculate those metrics, we first need to classify the events detected as: true positive (TP), false positive (FP), true negative (TN), and false negative (FN). True positive is the result of an

intrusion event that is succesfully detected by the IDS. False positive is the results of a non-intrusive event that is classified as intrusive by the IDS. True negative is the result of a non-intrusive event that is successfuly classified as non-intrusive. False negative is the result of intrusions that are classified as non-intrussive events. In this manner, the security metris are defined as:

- Classification rate is the ratio of correctly classified events and the total number of events. The classification rate is calculated as shown in Equation 1.

$$CR = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

- Detection rate is the ratio between the correctly detected attacks and the total number of attacks. The detection rate is calculated as shown in Equation 2.

$$DR = \frac{TP}{TP + FN} \quad (2)$$

- False positive rate is the ratio between the number of non-intrusive events classified as attack and the total number of non-intrusive events. The false positive ratio is calculated as shown in Equation 3.

$$FPR = \frac{FP}{FP + TN} \quad (3)$$

- Precision is the ratio of events classified as positive that are actually positive. The precisions is calculated as shown in Equation 4.

$$PR = \frac{TP}{TP + FP} \quad (4)$$

Finally, the parameters for simulations and testbed will be: topology sizes, number of intruders, position of intruders, level of the attack, number of HPP nodes, and number of controllers. The level of the attack is defined by the frequency of packets with false flows.

V. Conclusion

In this work we present a first research project to pursue a doctorate degree. This research is about security in SDWSN. We compare three IDS mechanisms to countermeasure a DoS attack where the intruder aims to saturate the nodes flow table and exhaust the SDN controller resources. Two of those mechanisms have a cooperative approach and the third one is totally centralized. We believe that due to resources constraints in SDWSN, the cooperative approach is the right solution to improve intrusion detection effectiveness without degrading the network performance.

Acknowledgment

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001. Cintia B. Margi is supported by CNPq fellowship (Pq) #307304/2015-9. Gustavo A. Nunez Segura is supported by Universidad de Costa Rica.

References

[1] KOBO, H. I.; ABU-MAHFOUZ, A. M.; HANCKE, G. P. A Survey on Software-Defined Wireless Sensor Networks: Challenges and Design Requirements. *IEEE Communications Surveys & Tutorials*, v. 3536, n. Submitted for publication, 2017. ISSN 2169-3536.

[2] MCKEOWN, N. et al. OpenFlow: enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review*, v. 38, n. 2, p. 69, 2008. ISSN 01464833. Disponível em: <http://portal.acm.org/citation.cfm?doid=1355734.1355746>.

[3] KREUTZ, D. et al. Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, v. 103, n. 1, p. 14–76, 2015. ISSN 00189219. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6994333>.

[4] MOSTAFAEI, H.; MENTH, M. Software-defined wireless sensor networks: A survey. *Journal of Network and Computer Applications*, v. 119, p. 42 – 56, 2018. ISSN 1084-8045. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1084804518302248>.

[5] TOMIć, I.; MCCANN, J. A. A survey of potential security issues in existing wireless sensor network protocols. *IEEE Internet of Things Journal*, v. 4, n. 6, p. 1910–1923, Dec 2017. ISSN 2327-4662.

[6] DABBAGH, M. et al. Software-defined networking security: pros and cons. *IEEE Communications Magazine*, v. 53, n. 6, p. 73–79, June 2015. ISSN 0163-6804.

[7] DUAN, Y. et al. Software defined wireless sensor networks: A review. In: *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD))*. [S.l.: s.n.], 2018. p. 826–831.

[8] PRITCHARD, S. W.; HANCKE, G. P.; ABU-MAHFOUZ, A. M. Cryptography methods for software-defined wireless sensor networks. In: *2018 IEEE 27th International Symposium on Industrial Electronics (ISIE)*. [S.l.: s.n.], 2018. p. 1257–1262. ISSN 2163-5145.

[9] AHMAD, I. et al. Security in software defined networks: A survey. *IEEE Communications Surveys Tutorials*, v. 17, n. 4, p. 2317–2346, Fourthquarter 2015. ISSN 1553-877X.

[10] AKHUNZADA, A. et al. Securing software defined networks: taxonomy, requirements, and open issues. *IEEE Communications Magazine*, v. 53, n. 4, p. 36–44, April 2015. ISSN 0163-6804.

[11] SHU, Z. et al. Security in software-defined networking: Threats and countermeasures. *Mobile Networks and Applications*, v. 21, n. 5, p. 764–776, Oct 2016. ISSN 1572-8153. Disponível em: <https://doi.org/10.1007/s11036-016-0676-x>.

[12] SCOTT-HAYWARD, S. Design and deployment of secure, robust, and resilient sdn controllers. In: *Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft)*. [S.l.: s.n.], 2015. p. 1–5.

[13] HU, T. et al. Multi-controller based software-defined networking: A survey. *IEEE Access*, v. 6, p. 15980–15996, 2018. ISSN 2169-3536.

[14] MARGI, C. et al. Segurança em redes de sensores sem fio. *Minicursos: SBSeg*, p. 149–194, 2009.

[15] AJAEIYA, G. A. et al. Flow-based intrusion detection system for sdn. In: *2017 IEEE Symposium on Computers and Communications (ISCC)*. [S.l.: s.n.], 2017. p. 787–793.

[16] SANGODOYIN, A. et al. An approach to detecting distributed denial of service attacks in software defined networks. In: *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*. [S.l.: s.n.], 2018. p. 436–443.

[17] GRIGORYAN, G. et al. Enabling cooperative iot security via software defined networks (sdn). In: *2018 IEEE International Conference on Communications (ICC)*. [S.l.: s.n.], 2018. p. 1–6. ISSN 1938-1883.

[18] LIAO, H.-J. et al. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, v. 36, n. 1, p. 16 – 24, 2013. ISSN 1084-8045. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1084804512001944>.

[19] DUNKELS, A.; GRONVALL, B.; VOIGT, T. Contiki-a lightweight and flexible operating system for tiny networked sensors. In: IEEE. *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*. [S.l.], 2004. p. 455–462.

[20] ALVES, R. C. A. et al. IT-SDN: Improved architecture for SDWSN. *XXXV Brazilian Symposium on Computer Networks and Distributed Systems*, 2017.

Modeling user trust and data quality in Citizen Science projects

Modelagem para determinação da confiança no usuário e qualidade de dados em projetos de *Citizen Science*

LEOCADIO, J. N.*; DADA, S. G.*; CARTOLANO-JÚNIOR, E. A.*; SARAIVA, A. M.*
*Laboratório de Automação Agrícola (LAA)
Núcleo de Pesquisa em Biodiversidade e Computação (BIOCOMP)
Departamento de Engenharia de Computação e Sistemas Digitais (PCS)
Escola Politécnica da Universidade de São Paulo (EPUSP)
E-mail: {jailsonleocadio, sheila.dada, cartolano, saraiva}@usp.br

***Abstract*—Citizen Science projects have been gaining popularity in biodiversity studies in several regions of the planet. With it, it is possible the monitoring of extensive areas and the registration of biological species that traditionally would require great effort, time and resources. However, the authors in scientific literature report several problems in the outcomes of these projects, such as the lack of ability to carry out the proposed activities, motivation, biases, data quality problems and the need for later data validation. Despite this, Citizen Science is a social movement that can contribute in many ways to science and biological biodiversity studies. Here we intend to create explanatory mathematical models for the individuals ability, learning and behavior to define trust by means of these parameters and to relate them to the quality of the data collected, in a data-driven analysis. We will use the expectations and evidence model to define what is expected of individuals and data and what characteristics in the final dataset is allow us to define the real situation of both. A purpose for using the data will be set for bias evaluation. We hope this study contributes to the definition of trust in citizen scientists and the quality of data produced and to guarantee applicability of the data to the objectives proposed in biodiversity studies.**

***Keywords*— Citizen Science; Data science; Trust; Data quality.**

***Resumo*— Os projetos de *Citizen Science* têm sido frequentes em estudos de biodiversidade em diversas regiões do planeta. Com ela é possível o monitoramento de extensas área e o registro de espécies biológicas que, tradicionalmente demandariam grande esforço, tempo e recursos. Contudo, os autores relatam diversos problemas na implementação desses projetos, como a falta de habilidade para a execução das atividades propostas, motivação, vieses, problemas de qualidade nos dados e necessidade de validação posterior. Apesar disso, *Citizen Science* é um movimento social que pode contribuir de inúmeras formas para a ciência e para os estudos da biodiversidade biológica. Aqui, pretendemos criar modelos matemáticos explicativos para a habilidade, aprendizado e comportamento dos indivíduos, definir a confiança neles através desses parâmetros e relacioná-los com a qualidade dos dados obtidos, numa análise *data-driven*. Utilizaremos o modelo de expectativas e evidências para definir o que se espera dos indivíduos e dos dados e quais as características no conjunto final dos dados permitiria definir a real situação de ambos. Um propósito de uso dos dados será definido para avaliação de vieses. Espera-se contribuir para a definição da confiança em *citizen scientists* e da qualidade do dados produzidos e para a possível aplicabilidade dos dados para os objetivos propostos nos estudos de biodiversidade.**

***Palavras-chave*— *Citizen Science*; Ciência de dados; Confiança; Qualidade de dados.**

***Classificação*— Doutorado**

***Categoria*— Iniciante**

I. INTRODUÇÃO

O envolvimento de cidadãos sem formação científica em projetos de pesquisa é denominado de *Citizen Science* (CS) e tem sido uma prática crescente nos últimos anos. Esse fato é apoiado, principalmente, pelas facilidades na produção, coleta e difusão de dados através das tecnologias de comunicação de uso cotidiano, como o *smartphone*, que possuem diversos sensores capazes de prover informações relevantes sobre o ambiente.

Na área de estudo de biodiversidade, *CS* tem se mostrado como uma alternativa que possibilita o monitoramento de extensas áreas naturais e o registro de inúmeras espécies biológicas, que de outra maneira seria inviável pela quantidade de recursos necessários, tempo e custos associados.

Contudo, diversos autores relatam problemas com essa prática. Uma das principais questões diz respeito à participação oportunística dos indivíduos envolvidos. Isso quer dizer que os dados obtidos apresentam vieses que correspondem às decisões dos participantes de quando e onde executar as

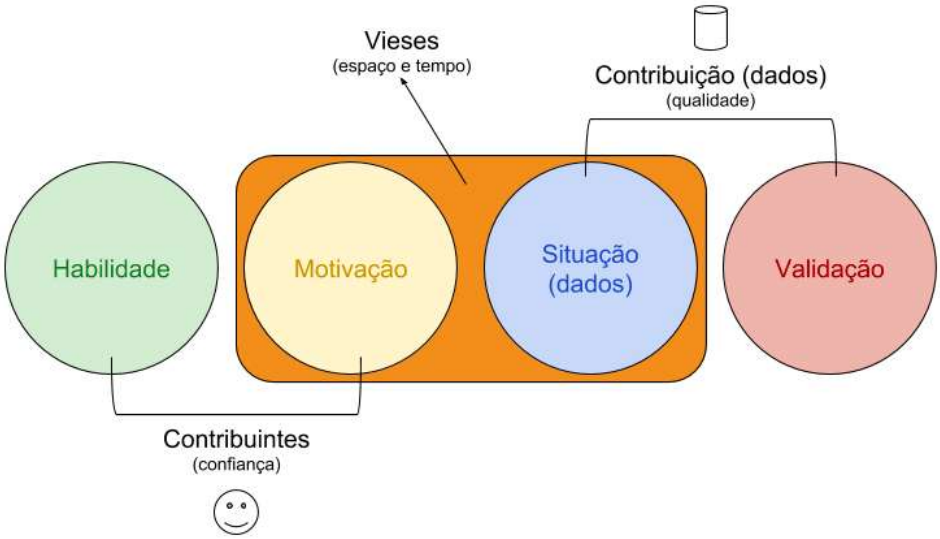


Figura 1. Síntese dos problemas apresentados na literatura acerca da aplicação de *Citizen Science* em estudos de biodiversidade.

atividades deles requerida. Por isso alguns autores informam que *CS* deveria ser utilizado apenas como uma ferramenta complementar [1] e para aumentar os dados os dados coletados por profissionais [2].

Embora problemas sejam frequentes nos projetos de *CS*, [3] conclui que eles são semelhantes àqueles encontrados nos dados coletados pela ciência tradicional. Além disso, a manipulação dos conjuntos de dados após as coletas, através de processos de tratamento e limpeza, podem minimizar e, possivelmente, corrigir os problemas encontrados [4], tornando-os prontos para a aplicação pretendida. Para [5], em um projeto de *CS* quando bem planejado e executado é possível obter resultados valiosos.

Os objetivos deste trabalho são de: fazer o levantamento dos principais problemas relacionados a *Citizen Science*, quando aplicado em estudos de biodiversidade e relatados na literatura; propor modelos matemáticos explicativos para a habilidade, aprendizado e comportamento dos indivíduos; definir a confiança neles através desses parâmetros; e relacioná-los com a qualidade dos dados obtidos, numa análise *data-driven*.

II. Mapeamento Sistemático

Na literatura, são encontrados relatos de diversos problemas na aplicação de *CS* e alguns deles serão tratados a seguir. No trabalho desenvolvido por [6], os autores destacaram a existência de dados duplicados, atrasos no envio de registros devido a problemas pessoais dos participantes, além de problemas relacionados à habilidade para utilizar os *softwares* necessários. Nesses casos, os problemas são de diferentes tipos: nas características dos dados coletados, de ordem pessoal e relativos à capacidade para desenvolvimento de tarefas.

Já no trabalho de [7], os principais problemas obtidos foram devidos à existência de custos, para os participantes, na realização das atividades. A motivação também foi outro fator observado que influenciou na execução das tarefas. Os autores destacam que em locais com população de menor poder aquisitivo, a adoção de projetos desse tipo pode ser prejudicada caso existam custos para os participantes e que, frequentemente, os conceitos de voluntariado nessas comunidades ainda não estão difundidos. Uma solução, nesse caso, seria a adoção de premiação para aumentar a motivação e o engajamento.

De maneira semelhante, [8] relata que é um desafio trabalhar com participantes com habilidades limitadas e relutantes no comprometimento em um monitoramento contínuo. Por isso são necessários treinamentos [9] para demonstrações e aprimoramento das técnicas requeridas e para apresentação dos protocolos padronizados de coleta de dados.

Para [10], como existem diversos níveis de habilidade e experiência entre os participantes, é preciso a implementação de um controle de qualidade dos indivíduos, que possa informar sobre a confiança sobre aquilo que é produzido por eles. É imprescindível a validação posterior dos dados [4].

Na figura 1 é apresentada uma síntese dos problemas apresentados pelos diversos trabalhos analisados. Destaca-se a classificação em dois principais grupos de mesmo nível: problemas relacionados aos participantes e relacionados aos dados. Essa divisão reflete a posição dos autores em destacar as características pessoais dos indivíduos que influenciam e diferenciam *CS* da prática tradicional científica e os dados por eles produzidos:

- Habilidade: diz respeito à capacidade do indivíduo em realizar a atividade que lhe é atribuída; por exemplo, em projetos que solicitam aos usuários o registro de observações de espécies, geralmente são requeridas habilidades para identificação de espécies;
- Motivação: está relacionada com o esforço empregado para a execução da atividade; por exemplo, quantas horas semanais está ativo na execução de coleta de dados ou quantas espécies foram observadas e/ou identificadas;

- Situação (dados): descrição do nível de qualidade dos dados obtidos pelos *citizen scientists*; por exemplo, através de dimensões como acurácia, completude, consistência, entre outras;
- Validação: processo para intervenção na situação dos dados com o objetivo de validação e melhoria; alguns autores citam como um processo indispensável e que traz mais custos para o projeto;
- Vieses: os vieses correspondem aos principais problemas relatados pelos autores, pois como as coletas de dados nem sempre seguem um protocolo restrito, carregam diversas variações inseridas pelo comportamento dos indivíduos e ferem princípios da prática científica.

De modo geral, a síntese de problemas proposta pode ser assim entendida: os indivíduos apresentam, previamente, uma determinada habilidade para execução das atividades que lhe são solicitadas e isso é variável entre os participantes; a motivação determina a quantidade de esforço desprendido nas atividades; com o passar do tempo, a experiência melhora a habilidade, o que caracteriza aprendizagem; de modo semelhante, o conjunto de dados coletados apresenta uma caracterização inicial, definida pelo nível de qualidade encontrado; o processo de validação pode melhorar a qualidade deles e torná-los mais apropriados para uso; já os vieses são encontrados no esforço empregado pelo indivíduo, como a escolha do momento e local de coleta de dados, e são transferidos para os dados em si, ou seja, os dados podem apresentar autocorrelações devido ao comportamento dos participantes.

Para avaliação da qualidade dos dados, comumente se utiliza diversas dimensões para descrever as expectativas que se têm sobre os dados, como acurácia, completude, consistência, entre outros. No trabalho de [11], os autores analisaram as características dos voluntários (idade e conhecimento prévio) que poderiam afetar a qualidade dos dados, em termos de padronização, acurácia, precisão, representação temporal e espacial e tamanho das amostras e ao final, fizeram recomendações para aumentar a qualidade.

III. Trabalhos Relacionados

No trabalho desenvolvido por [12], os autores utilizaram um Modelo Misto Aditivo Generalizado (GAMM) para explicar a habilidade do usuário em realizar as atividade de detecção e identificação de aves (Figura 2) no projeto e-Bird[1]. Nesse projeto, os participantes realizam saídas de campo para observação de aves e fazem registros das espécies que são encontradas. Posteriormente, enviam para a base de dados do projeto, informações como: data e hora da atividade, localização, lista das espécies observadas, tempo empregado, se durante a atividade manteve-se parado ou em movimento, distância percorrida, entre outras.

No modelo apresentado, as diversas variáveis que o compõe foram classificadas em três grupos: as que explicam o número de espécies presentes no local e na data da coleta (período do ano, localidade e *habitat*), afetam a probabilidade de um

[1]https://ebird.org

$$\log(N_k) = \alpha_0 + \alpha_1 hrs_k + \alpha_2\sqrt{hrs_k} + \sum_{j=1}^{14}\beta_j land_{j,k} + \beta_{15} GS_k + f_1(day_k) + \gamma_1 protocol_k + \gamma_2 dist.km_k + \gamma_3 no.observers_k + f_2(time_k) + \delta_{1i} + \delta_{2i} hrs_k + \lambda_1 \log(checklist.no_{i,k}) + \varepsilon_k$$

$$\delta_{1i} \sim N(0, \sigma_1)$$
$$\delta_{2i} \sim N(0, \sigma_2)$$

Figura 2. Modelo. matemático explicativo proposto por [12].

usuário em encontrar uma espécie (período do dia, distância percorrida, número de observadores e tempo desprendido) e a habilidade do participante em detectar e identificar as espécies (variação média entre todos os usuários e efeitos randômicos). Em conjunto com o uso de Curvas de acumulação de espécies (SAC), estimaram o número de espécies reportado por um observador.

No trabalho, os autores avaliaram variações inter e intra observadores, além do processo de melhoria da habilidade individual ao longo do tempo. Os resultados obtidos apontaram importantes análises para o caso específico: o número de espécies aumenta com a experiência; *expertise* não é somente detectar espécies mais raras e sim detectar taxas elevadas de todas as espécies; existências de diversos grupos de usuários com habilidade e comportamentos semelhantes. Como conclusão, eles ressaltam que o estudo sobre as variações de habilidade entre os indivíduos melhora as inferências feitas a partir dos dados.

IV. Metodologia

Para este trabalho, classificaremos os problemas acerca dos indivíduos (habilidade e motivação) como fatores que determinam a confiança do usuário; semelhantemente, problemas acerca dos dados (situação e validação) serão considerados como determinantes para a qualidade dos dados. Utilizaremos o modelo proposto por [13], que determina que a confiança é uma função de expectativas e evidências. Dessa forma, primeiro se define quais são as expectativas sobre os indivíduos, ou seja, quais características determinam as habilidades desejadas, posteriormente são definidas quais as características dos dados são evidências das expectativas. Esse mesmo modelo será aplicado para estudo da qualidade do conjunto dos dados: as expectativas são as dimensões de qualidade.

Algumas das etapas de desenvolvimento são:

1) Selecionar projeto de *Citizen Science* para estudo;
2) Descrever as atividades e habilidades requeridas aos participantes;
3) Selecionar quais evidências, dentro do conjunto de dados produzidos, são capazes de descrever a habilidade dos participantes;
4) Avaliar as alterações de habilidade ao longo do tempo (aprendizagem);

5) Selecionar quais evidências descrevem as expectativas de qualidade dos dados obtidos, através do uso de dimensões de qualidade;
6) Definir uma aplicação para uso dos dados, como por exemplo, modelagem de distribuição de uma dada espécie ou estudo de riqueza de espécie numa determinada região;
7) Selecionar quais evidências apontam para os vieses presentes no conjunto total dos dados, de acordo com a aplicação definida;
8) Determinar o nível de confiança em um determinado usuário, a partir da determinação da habilidade e da qualidade dos dados por ele produzidos;
9) Indicar melhorias para aumentar a confiança nos usuários e a qualidade dos dados do projeto.

As etapas listadas acima informam sobre o processo de escolha do projeto, das variáveis de estudo e de possíveis análises a serem realizadas. O projeto de pesquisa, como um todo, estará incluído dentro de um ciclo de vida de dados, que inclui, resumidamente, etapas de pré-processamento da base de dados a ser manipulada, transformação dos dados, aplicação dos algoritmos para criação dos modelos e interpretação dos resultados.

V. Resultados Esperados

Os principais resultados esperados são:

- Mapeamento com descrição e classificação dos problemas comumente encontrados nos projetos de *CS* aplicados em estudos de biodiversidade, apoiado pela literatura;
- Definição das expectativas e evidências que determinarão a confiança do usuário e a qualidade de dados;
- Modelos explicativos que incluem em sua estrutura a habilidade, motivação, aprendizagem e comportamento dos indivíduos para determinação da confiança em um determinado usuário e da qualidade de dados por ele produzido.

Agradecimentos

Agradecemos à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo recurso financeiro concedido.

Referências

[1] LODI, L.; TARDIN, R. Citizen science contributes to the understanding of the occurrence and distribution of cetaceans in southeastern Brazil – A case study. *Ocean and Coastal Management*, v. 158, p. 45–55, 2018. ISSN 09645691. Disponível em: <https://doi.org/10.1016/j.ocecoaman.2018.03.029>.

[2] EDWARDS, P.; SHALOUM, G.; BEDELL, D. A unique role for citizen science in ecological restoration: a case study in streams. *Restoration Ecology*, v. 26, n. 1, p. 29–35, 2018. ISSN 10612971. Disponível em: <https://doi.org/10.1111/rec.12622>.

[3] THEOBALD, E. J. et al. Global change and local solutions: Tapping the unrealized potential of citizen science for biodiversity research. *BIOLOGICAL CONSERVATION*, v. 181, p. 236–244, jan. 2015. ISSN 0006-3207. Disponível em: <https://doi.org/10.1016/j.biocon.2014.10.021>.

[4] VUKELIC, M. et al. A cetacean monitoring system that integrates citizen science and satellite imagery. *RENDICONTI LINCEI-SCIENZE FISICHE E NATURALI*, v. 29, n. 1, p. 53–59, mar. 2018. ISSN 2037-4631. Disponível em: <https://doi.org/10.1007/s12210-017-0657-4>.

[5] ZENG, Q.; WEI, Q.; LEI, G. Contribution of citizen science towards cryptic species census: "many eyes" define wintering range of the Scaly-sided Merganser in mainland China. *AVIAN RESEARCH*, v. 9, fev. 2018. ISSN 2053-7166. Disponível em: <https://doi.org/10.1186/s40657-018-0098-5>.

[6] SLADONJA, B.; POLJUHA, D. Citizen Science as a Tool in Biological RecordingA Case Study of Ailanthus altissima (Mill.) Swingle. *FORESTS*, v. 9, n. 1, jan. 2018. ISSN 1999-4907. Disponível em: <https://doi.org/10.3390/f9010031>.

[7] WEESER, B. et al. Citizen science pioneers in Kenya – A crowdsourced approach for hydrological monitoring. *Science of the Total Environment*, v. 631-632, p. 1590–1599, 2018. ISSN 00489697. Disponível em: <https://doi.org/10.1016/j.scitotenv.2018.03.130>.

[8] GRASON, E. et al. Citizen science program detects range expansion of the globally invasive European green crab in Washington State (USA). *Management of Biological Invasions*, v. 9, n. 1, p. 39–47, 2018. ISSN 19898649. Disponível em: <https://doi.org/10.3391/mbi.2018.9.1.04>.

[9] WELDEN, N. A.; WOLSELEY, P. A.; ASHMORE, M. R. Citizen science identifies the effects of nitrogen deposition, climate and tree species on epiphytic lichens across the UK. *ENVIRONMENTAL POLLUTION*, v. 232, p. 80–89, jan. 2018. ISSN 0269-7491. Disponível em: <https://doi.org/10.1016/j.envpol.2017.09.020>.

[10] HORNS, J.; ADLER, F.; SEKERCIOGLU, C. Using opportunistic citizen science data to estimate avian population trends. *Biological Conservation*, v. 221, p. 151–159, 2018. ISSN 00063207. Disponível em: <https://doi.org/10.1016/j.biocon.2018.02.027>.

[11] LEWANDOWSKI, E.; SPECHT, H. Influence of volunteer and project characteristics on data quality of biological surveys. *Conservation Biology*, Blackwell Publishing Inc., v. 29, n. 3, p. 713–723, 2015. ISSN 08888892. Disponível em: <https://doi.org/10.1111/cobi.12481>.

[12] KELLING, S. et al. Can Observation Skills of Citizen Scientists Be Estimated Using Species Accumulation Curves? *PLOS ONE*, v. 10, n. 10, p. e0139600, out. 2015. ISSN 1932-6203. Disponível em: <https://doi.org/10.1371/journal.pone.0139600>.

[13] CARTOLANO, E.; SARAIVA, A. M.; STEVENSON, R. D. Playground 2.0: Simulating behavior decisions with trust and control computations. In: *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. [s.n.], 2016. p. 400–406. Disponível em: <https://doi.org/10.1109/PST.2016.7906963>.

AnimalMoveMiner: a spatial-temporal strategy to discovery of interaction between animal and environment
AnimalMoveMiner: uma estratégia para descoberta de interação espaço-temporal entre animais e meio ambiente

Suelane Garcia Fontes[1], Pedro Luiz Pizzigatti Corrêa[1], Silvio Luiz Stanzani[2]
[1]Escola Politécnica da Universidade de São Paulo – USP - São Paulo – SP – Brasil
[2] Centro de Computação Científica – UNESP - São Paulo – SP – Brasil
{suelane, pedro.correa}@usp.br, silvio@ncc.unesp.br

Resumo — ***Os avanços tecnológicos aumentaram a capacidade de monitorar, estudar e gerenciar os movimentos dos animais, fornecendo informações que podem ser usadas para identificar padrões de comportamento animal. O comportamento animal pode ser usado como base para a descoberta e entendimento da relação entre os animais e o meio ambiente.***
Este artigo apresenta uma estratégia, que combina algoritmos, para a descoberta de interação entre conjuntos de animais e, entre animais e os fatores ambientais ao longo do tempo e espaço. Foi realizada uma avaliação com um conjunto de dados de movimentação de onças-pintadas da Estação Ecológica de Taiamã, norte do Pantanal, Brasil, que apresentou, a interação entre onças e, entre o comportamento das onças e os diferentes cenários caracterizados pelas estações do ano e os períodos do dia (dia/noite).
Palavras-chave – ***data science, data mining*, trajetórias, dados espaço-temporais, comportamento animal.**
Classificação*— *Doutorado
Categoria— Em conclusão

I. INTRODUÇÃO

Os dados espaço-temporais relativos ao movimento animal, obtidos por meio de dispositivos móveis, estão sendo utilizados no monitoramento da fauna com a finalidade de fornecer informações sobre o comportamento animal que orientem ações e políticas de preservação e conservação da biodiversidade [1]. Em Ecologia [2], o comportamento animal é a base para entender a relação entre as espécies e o meio ambiente.

O movimento animal é o caminho percorrido pelo animal ao longo do espaço em um determinado período de tempo e é representado por pontos que determinam a posição (latitude/ longitude) e o tempo (data/hora) do movimento. Instituições, como a *United States Geological Survey* (USGS) e o Instituto Chico Mendes de Conservação da Biodiversidade (ICMBIO) utilizam a movimentação de animais nas pesquisas sobre mudanças ambientais.

Desta forma, a contribuição deste trabalho é fornecer uma estratégia para a descoberta de interações entre animais e, entre animais e os fatores ambientais ao longo do tempo e espaço utilizando dados da movimentação animal.

II. DEFINIÇÃO DO PROBLEMA E CONCEITOS

Nesta seção são apresentados o problema e os conceitos que norteiam este trabalho.

*Problema: c*om base na distribuição dos dados espaço-temporais, relativos à movimentação animal, pode-se obter padrões de comportamento dos animais e identificar quais fatores ambientais ocorreram próximos ao animal ao longo do tempo e espaço. Desta forma, o desafio é explorar os dados de movimentação animal e de fatores ambientais de forma a descobrir a interação entre animais e, entre animais e os fatores ambientais, classificando estas relações.

Conceitos

A análise exploratória do movimento animal é a base para a descoberta de padrões de comportamento, que representem o modo como o animal interage com o ambiente, por meio de fatores ambientais, tais como: temperatura, estações do ano, períodos do dia (dia/noite) ou presença de outros animais.

O movimento animal é a variação da posição espacial de um objeto em relação a um referencial no período de tempo, gerando um caminho representado por uma série de pontos ordenados no tempo, a trajetória. A análise de trajetórias [3] pode fornecer informações sobre por que, como, quando e onde os animais se movem e sua relação com o ambiente [4]. O movimento animal possui características como velocidade, tempo de residência, direção e distância percorrida ou a frequência de ocorrência que permitem identificar padrões de comportamento animal. O comportamento representa a parte de um organismo por meio do qual ele interage com o ambiente [5] e divide-se em: estados, ocorre por um período prolongado, exemplo, repouso, trânsito; eventos, contados ao longo do tempo, exemplo, lutando, perseguindo e desviando.

Métodos de segmentação são utilizados para particionar as trajetórias baseadas nas características do movimento, determinando os pontos de mudança do comportamento animal que indicam o local e o momento (latitude/longitude/ data/hora) da transição do comportamento [6].

O movimento animal ocorre em uma determinada área e pode ser influenciado por outros objetos que estão no mesmo ambiente, podendo ocorrer relações, tais como, de: similaridade, que é a distância entre trajetórias e pontos vizinhos; co-ocorrência, que representa subconjuntos de eventos que ocorrem juntos no espaço e no tempo; correlação [7], que é a relação de dependência entre duas ou mais variáveis ocorrendo no mesmo espaço e tempo.

III. ANIMALMOVEMINER

Nesta seção é apresentada a estratégia AnimalMoveMiner que permite a descoberta de interação entre animais e, entre animais e fatores ambientais ao longo do tempo e espaço. Por interação entende-se a correlação entre o comportamento

animal e os fatores ambientais ao longo do espaço e do tempo. Para a aplicação da estratégia deve-se fornecer como entrada: dados espaço-temporais relativos ao movimento de um ou mais animais caracterizados por: pontos (latitude/ longitude), tempo (data/hora) e nome do animal; dados espaço-temporais do fator ambiental, contendo o nome, posição (latitude/longitude), tempo (data/hora) e o status, exemplo, a classificação da temperatura (alta/baixa).

A estratégia permite que sejam realizadas análises com base em intervalos de valores para os parâmetros de entrada:

- Distância limite (TD) (metros): determina o tamanho do raio em torno de cada ponto (latitude/longitude) a ser considerado na análise da distância entre pontos relativos ao movimento animal e ocorrência dos fatores ambientais;
- Intervalo de tempo (TI): intervalo em minutos, usado para calcular a faixa de ocorrência do fator ambiental;
- Suporte Mínimo (SupM): mínima frequência (%) de ocorrência que duas variáveis devem ter juntas para que sejam consideradas relevantes na análise de correlação;
- Confiança Mínima (ConfM): mínima (%) probabilidade de uma variável ocorrer dada a ocorrência de outra

Quanto menor o valor de SupM e ConfM mais relações entre variáveis são recuperadas, no entanto, serão mostrados inclusive encontros raros entre os animais. Já quanto maior o valor de SupM e ConfM maior será o filtro das relações, mostrando somente as com maior probabilidade de ocorrerem juntas, apresentando maior correlação.

A estratégia AnimalMoveMiner possui três etapas, fig. 1, que são: Etapa A - identificar o comportamento animal; Etapa B - identificar os fatores ambientais vizinhos da ocorrência do comportamento animal; Etapa C - identificar a correlação entre o comportamento animal e fatores ambientais vizinhos.

Etapa A. Identificar o comportamento animal

Nesta etapa os dados espaço-temporais relativos ao movimento animal são analisados para identificar os pontos de mudança do comportamento animal que são os estados; os intervalos de ocorrência dos estados (hora início/fim), períodos frequentes e duração por comportamento, *outliers* dos períodos e *home range*.

O método RST [8] é usado para identificar os pontos de mudança no comportamento animal segmentando a trajetória com base na quantidade de espaço e tempo ocupados pelo animal em uma área de escala constante. Em torno de cada ponto do movimento animal é construído um círculo, de acordo com o TD, e é calculada a distância percorrida RD e o tempo gasto RT entre pontos consecutivos dentro do círculo. Os valores RD e RT são normalizados dividindo-se pelo valor máximo do mesmo dentro de cada faixa, obtendo como resultado um intervalo entre 0 e 1 de resíduo. Para cada ponto da trajetória o comportamento animal é classificado como: descanso (resíduo < 0): um tempo alto na área, mas uma curta distância percorrida; trânsito (resíduo = 0): baixo tempo e distância na área; forragem (resíduo > 0): alto tempo e distância na área.

Com base na movimentação animal os períodos (hora início/término) de ocorrência do estado do comportamento animal por dia, mês e ano são identificados, gerando intervalos entre horas e a duração de cada período por estado. A duração dos períodos é a base para identificar os *outliers* dos períodos, por meio do pacote outliers [9] e removê-los dos dados. Os outliers são registros de duração do estado de comportamento que diferem fortemente de todos os outros e podem causar anomalias nos resultados das análises.

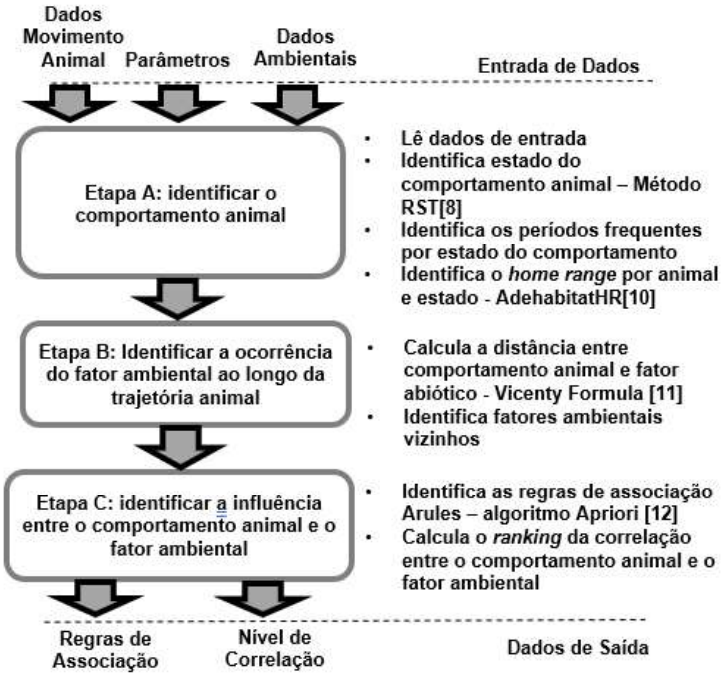


Fig. 1 – Etapas e Recursos da Estratégia – AnimalMoveMiner

Para identificar os períodos frequentes, primeiro são identificados os intervalos de hora (início/fim) que, freqüentemente, ocorrem para cada estado. Segundo, identifica-se a sobreposição de períodos formando novos períodos com as intersecções.

Para identificar a área de vida, *home range*, dos animais por estado de comportamento, mês e ano, utiliza-se a função kernelUD [10], que fornece a densidade de probabilidade de um animal ser encontrado em um ponto de acordo com suas coordenadas geográficas, que corresponde à área mínima em que um animal tem probabilidade de ser localizado. O *home range* permite identificar as áreas ocupadas pelos animais ao longo do tempo.

Etapa B. Identificar os fatores ambientais vizinhos da ocorrência do comportamento animal

Os dados do movimento animal e dos fatores ambientais são analisados para identificar os fatores presentes ao longo do movimento animal. Duas situações são consideradas: fatores que possuem informações sobre espaço (latitude/ longitude) e tempo, onde calcula-se a distância entre o fator e o movimento animal e, a segunda situação, onde os fatores estão na área do movimento animal, mas há somente informações sobre tempo. Na primeira situação, é realizada a análise da distância entre ambos e a sincronização da data/hora, considerando o acréscimo de uma margem em minutos, parâmetro TI, antes e depois das horas de início e fim para recuperar as ocorrências dos fatores. No cálculo da distância é usada a fórmula de Vicenty [11], então para cada registro do movimento animal cria-se um círculo em torno deste ponto (posição e tempo) com raio de distância igual ao TD e calcula-se a distância. Na segunda situação, utiliza-se a data/hora para explorar os dados. A data de movimentação é sincronizada com a data do fator ambiental, considerando acréscimo de TI, antes e depois, para calcular o intervalo de hora para recuperar os fatores ambientais.

Etapa C. Identificar a correlação entre comportamento animal e fatores ambientais vizinhos

Nesta etapa, são definidas as variáveis a serem analisadas e a técnica de regras de associação é aplicada para identificar a correlação entre as variáveis. Esta regra encontra elementos que impliquem na presença de outros elementos na mesma transação indicando a freqüência de co-ocorrência dos elementos por meio do algoritmo Apriori [12]. Os dados de entrada para o Apriori são: ao menos duas variáveis de status, referentes ao comportamento e fator ambiental, e os valores SupM e ConfM. O Apriori identifica as regras de associação entre as variáveis A e B, considerando a frequência com que ocorrem em conjunto e eliminando as regras que estão abaixo dos limites mínimos de SupM e ConfM. Como resultado, são obtidas as regras de associação e as medidas que identificam a correlação e dependência entre as variáveis analisadas [13].

As medidas obtidas indicam a frequência de co-ocorrência (**Sup**) das duas variáveis (A e B); a frequência de ocorrência somente da variável A (**SupA**); a frequência somente da variável B (**SupB**); a frequência esperada (**SupEsp**) de co-ocorrência das variáveis A e B, calculada pela multiplicação de **SupA** por **SupB**; e a confiança (**Conf**), que indica a probabilidade de B ocorrer em função da ocorrência da variável A.

Outras medidas que indicam a dependência entre as variáveis A e B também são obtidas. A dependência positiva indica que a presença de uma variável aumenta a presença de outra. A dependência negativa indica que a presença de uma variável diminui a presença de outra. Independentes, indica que uma variável não influencia na presença de outra. As medidas são:

- **Lift (L),** que classifica a dependência como: **L > 1,** A tem efeito sobre B (valor = 1); **L < 1,** A tem efeito negativo em B (valor = -1); **L = 1,** A e B independentes. B não tem efeito em A (valor = 0);
- **SupDep**, que classifica a dependência com base no **SupA** e **SupEsp**, como: Sup > SupEsp, dependência positiva (valor = 1); Sup < SupEsp, dependência negativa (valor = -1); Sup = SupEsp, independentes (valor = 0);
- **ConfDep**, que classifica a dependência com base no **Conf** e **SupB**, como: Conf(A-B) > SupB, dependência positiva (valor = 1); Conf(A-B) < SupB, dependência negativa (valor = -1); Conf(A-B) = SupB, independentes (valor = 0)

Outra medida obtida é o coeficiente de correlação **(Phi)** que indica a força da relação entre A e B, classificando o nível de correlação entre as variáveis [14], como: correlação negativa perfeita (-1); forte correlação negativa (-1.0 a -0.68); moderada correlação negativa (-0.67 a -0.36); fraca ou nenhuma correlação (-0.35 a 0.35); moderada correlação positiva (0.36 a 0.67); forte correlação positiva (0.68 a 1.0); sem correlação (0); correlação positiva perfeita (1).

Com base nas regras de associação e medidas obtidas, a última etapa da estratégia é classificar (ranking), usando a fórmula:

LCorr = ConfDep (valor) + SupDep (valor) + phi (valor) + Lift (valor)

A classificação é definida somando-se as medidas que indicam a dependência entre as variáveis, que são os valores de confDep, SupDep e Lift e o nível de correlação definido pelo valor de phi.

IV. AVALIAÇÃO E DISCUSSÃO

Nesta seção é apresentada a avaliação realizada com a estratégia proposta, utilizando um conjunto de dados referente ao movimento de nove onças-pintadas que residem na região da Estação Ecológica de Taiamã, norte do Pantanal, Brasil, coletadas via colar GPS, de 2013 a 2015. O conjunto de dados contém informações sobre a posição (latitude/ longitude) e a hora (data/hora) do movimento do animal.

Para a definição dos parâmetros de entrada foram realizadas análises preliminares com os dados de movimentação animal, utilizando diferentes valores para os parâmetros. Um exemplo dos valores utilizados é o TD igual a 400 metros, que é um valor intermediário de distância. O SupM e ConfM foram definidos com valores baixos para a obtenção, inclusive das relações menos frequentes entre as variáveis analisadas. O TI foi definido para 10 minutos antes/depois como uma forma de recuperar somente ocorrências com horários bem próximos das ocorrências analisadas.

Foram realizados dois estudos: primeiro, com foco na descoberta de interação entre as onças-pintadas; e o segundo, na interação entre comportamento das onças e o ambiente, baseado nos diferentes cenários caracterizados pelas estações do ano. Em ambos os estudos de casos os dados espaço-temporais referentes à movimentação dos animais e às ocorrências dos fatores ambientais foram analisados aplicando as três etapas da estratégia.

Para o primeiro estudo, na tabela 1, é mostrada uma parcial dos resultados obtidos com a análise da correlação entre os animais. Os resultados indicam a interação, em Fev/2015, entre as onças Caiman e Fera, apresentando correlação positiva. No entanto, o percentual de correlação entre estes animais é baixo, porque a frequência de ocorrência juntos foi baixa. Caiman e Dale, também apresentaram correlação positiva em Fev/2015, com 11 encontros.

Tabela 1. Correlação entre Onças

Ano 2015	Animais		% correlação	Total Ocorrência	Indicativo
Fev	Caiman	Fera	0,35	1	correlação positiva
Fev	Dale	Caiman	0,51	11	correlação positiva
Jan	Dale	Anderson	0	2	Não correlacionado

Estas interações podem ser observadas também no mapa de *home range* dos animais, identificado por estado, mês e ano. No caso de Caiman e Fera, fig. 2, é verificada a sobreposição do *home range* dos dois animais em Fev/2015, sendo em cinza mais escuro o *home range* da onça Fera e a parte em cinza claro o *home range* da onça Caiman. Como Caiman apresentou interação com Fera e Dale em Fev/2015, pode-se observar a interação entre os três por meio da sobreposição do home range das três onças. Os resultados também indicaram os animais não correlacionados, como Dale e Anderson, em Jan/2015, que apesar de terem duas ocorrências de encontro não estão correlacionados, indicando que mesmo ocorrendo encontros a ocorrência de um animal pode não influenciar a ocorrência do outro. No mapa de *home range*, fig. 3, de Jan/2015, observa-se que a área ocupada pela onça Dale não sobrepõe a área ocupada pela onça Anderson.

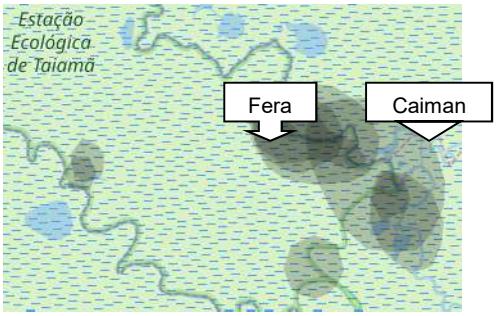


Fig. 2 – Home Range – onças Caiman e Fera

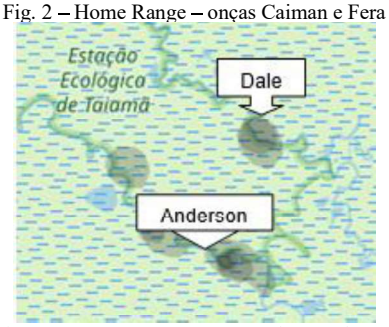


Fig. 3 – Home Range – onças Dale e Anderson

Para o segundo estudo, foi analisada a interação entre o comportamento de forrageamento das onças e o ambiente, baseado em diferentes cenários caracterizados pelas estações do ano da Região de Taiamã e os períodos do dia (dia/noite).

O clima na região pode ser dividido em quatro estações distintas[15]: seca (junho a setembro), enchente (outubro a dezembro), cheia (janeiro a março) e baixa (abril a maio). As chuvas concentram-se nos meses de dezembro, janeiro e fevereiro.

Como resultado do estudo foram obtidos os percentuais de ocorrência do forrageamento para cada onça por período do dia (dia/noite) e estação do ano, tabela 2. Observa-se que para 2015, os percentuais de frequência de forrageamento das onças indicam uma tendência das onças forragearem durante a noite independente da estação do ano.

Tabela 2. Interação entre forrageamento e períodos e estações - Ano 2015

Estações	Alice	Anderson	Caiman	Dale	Fera	Picole
Enchente						
Cheia	N = 54,76% D = 38,10%	N = 31,45% D= 7,26%	N = 64,29% D = 35,71%	N = 50,62% D = 14,81%	N = 25,00% D = 14,84%	N = 35,23% D = 37,50%
Baixa	N = 7,14%	N = 21,77% D = 8,87		N = 25,93% D = 8,64%	N = 18,75% D = 2,34%	N = 17,05% D = 10,23%
Seca		N = 23,39% D = 7,26			N = 31,25% D = 7,81%	
Ano: 2015 | Legenda: D: Dia N: Noite						

Outra observação, tabela 3, é que os meses com registro de maior duração do forrageamento, para cada onça, são relativos à estação de cheia, indicando que as onças passam maior parte do tempo forrageamento nesta estação.

Tabela 3. Interação entre forrageamento e duração do estado e estações.

2015	Meses com maior tempo de duração do forrageamento
Alice	Jan/Mar (Cheia)
Picole	Jan/Fev (Cheia) - Mai (Baixa)
Dale	Jan (Cheia) - Abr (Baixa)
Caiman	Fev (Cheia)
Fera	Fev - (Cheia) / Ago (Seca)

V. Conclusão

Neste artigo foi mostrada a estratégia AnimalMoveMiner que tem como objetivo permitir a descoberta de interações entre conjuntos de animais e, entre animais e os fatores ambientais ao longo do tempo e espaço, utilizando dados da movimentação animal

Com a aplicação da estratégia, por meio dos estudos, no contexto da área de biodiversidade e com a análise dos resultados obtidos, foi possível verificar a viabilidade e a contribuição da estratégia proposta no que tange a descoberta de interação entre animais e o meio ambiente ao longo do tempo e espaço.

Agradecimentos

Este estudo foi financiado em parte pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) - Código Financeiro 001. Agradecemos à Universidade de São Paulo (EPUSP) e à Estação Ecológica ICMBio - Taiamã, com especial atenção aos analistas ambientais, Daniel Kantek, Selma Onuma e Thadeu Pereira e, o ICMBIO-CENAP pelo fornecimento dos dados de Taiamã, em especial ao analista ambiental Ronaldo Morato.

Referências

[1] Kanda, Claudia Zukeran et al. Contribuição da geotecnologia no planejamento para a conservação da onça-pintada no Pantanal sul do Brasil. 8º Congresso de extensão universitária da UNESP, p. 1-5, 2015. Disponível em: <http://hdl.handle.net/11449/142675>.

[2] SCOTT, G. **Essential Animal Behavior**. John Wiley & Sons, 2009.

[3] DEMŠAR, U. *et al.* Analysis and visualisation of movement: an interdisciplinary review. **Movement Ecology**, 2015. v. 3, n. 1, p. 5.

[4] PHAN, N. **Mining Object Movement Patterns from Trajectory Data**. [S.l.]: Université Monpellier 2, 2013. phdthesis. Disponível em: <https://hal-lirmm.ccsd.cnrs.fr/tel-01379206/document>. Acesso em: 5 fev. 2018.

[5] SNOWDON, C. T. O significado da pesquisa em Comportamento Animal. **Estudos de Psicologia (Natal)**, dez. 1999. v. 4,p. 365–373.

[6] EDELHOFF, H.; SIGNER, J.; BALKENHOL, N. Path segmentation for beginners: an overview of current methods for detecting changes in animal movement patterns. **Movement Ecology**, dez. 2016. v. 4.

[7] MARI, D. D.; KOTZ, S. **Correlation and Dependence**. [S.l.]: Imperial College Press, 2001.

[8] TORRES, L. G. *et al.* Classification of Animal Movement Behavior through Residence in Space and Time. **PLOS ONE**, 3 jan. 2017. v. 12, n. 1, p. e0168513.

[9] KOMSTA, L. Outliers package | R Documentation. [S.l.], [s.d.]. Disponível em: <https://www.rdocumentation.org/packages/outliers/versions/0.14>. Acesso em: 12 nov. 2018.

[10] CALENGE, C. Analysis of animal movements in R: the adehabitatLT Package. 2015.

[11] VINCENTY, T. Direct and Inverse Solutions of Geodesics on the Ellipsoid with Application of Nested Equations. **Survey Review**, 1 abr. 1975. v. 23, n. 176, p. 88–93.

[12] HAHSLER, M.; GRUEN, B.; HORNIK, K. arules – A Computational Environment for Mining Association Rules and Frequent Item Sets. **Journal of Statistical Software**, out. 2005. v. 14, n. 15, p. 1–25.

[13] MANIMARAN, J.; VELMURUGAN, T. Analysing the Quality of Association Rules by Computing an Interestingness Measures. **Indian Journal of Science and Technology**, 15 jul. 2015. v. 8, n. 15. Disponível em: <http://www.indjst.org/index.php/indjst/ article/view/76693>. Acesso em: 25 set. 2017.

[14] TAYLOR, R. Interpretation of the Correlation Coefficient: A Basic Review. **Journal of Diagnostic Medical Sonography**, jul. 2016. v. 6, p. 35–39.

[15] ICMBIO. **Plano de Manejo da Estação Ecológica de Taiamã**. Disponível em: <http://www.icmbio.gov.br/portal/images/stories/plano-de-manejo/plano_de_manejo_esec_taiama_vs_070617.pdf>. Acesso em: 28 set. 2018.

Managing Architecture Decisions in Collaborative Environments of Software-Centric Architecture Gerenciando Decisões Arquiteturais em Ambientes Colaborativos de Produção de Software Centrados em Arquitetura

ROSSI, A. C.*; HIRAKAWA, A. R.†; BECERRA, J. L. R. *
*Laboratório de Tecnologia de Software - Universidade de São Paulo
†Laboratório de Sistemas Aberto/Smart Universidade de São Paulo
E-mail: {ana.rossi, ahirakawa, jorge.becerra}@usp.br

***Abstract*—The activities of the process of production and evolution of software systems involve activities that are intensively based on knowledge. However, knowledge management, more specifically, architectural knowledge management is a field of research that has many open problems and research opportunities. The software architecture is pointed out in the literature as a very important element in the life cycle of a software system, from the design, construction, evolution and discontinuity of the software system. In this sense, the purpose of this paper is to validate the use of the RM-ODP (Reference Model for Open Distributed) standard correspondence model to allow the traceability of the interested parties' interests and the modification and evolution generated in the elements that describe the software architecture in the different architectural visions. The contribution of the research is related to evolution and sustainability of the software architecture in the context of architecture-centric software production environment.**

***Keywords*— software architecture; architectural knowledge; architecture-centric Process; RM-ODP.**

***Resumo*— Os processos envolvidos na produção e evolução de sistemas de software envolvem atividades que são intensivamente baseadas em conhecimento. Entretanto, gerenciamento do conhecimento, mais especificamente, o gerenciamento do conhecimento arquitetural ainda é um campo de pesquisa que possui muitos problemas em aberto e oportunidades de pesquisa. A arquitetura de software é apontada na literatura como um elemento muito importante no ciclo de vida de um sistema de software, desde a concepção, construção, evolução e descontinuidade do sistema de software. Neste sentido, o objetivo deste trabalho é validar o uso do modelo de correspondências do padrão RM-ODP (Reference Model for Open Distributed) para permitir a rastreabilidade dos interesses das partes interessadas e as modificações e evoluções geradas nos elementos que descrevem a arquitetura de software nas diferentes visões arquiteturais. A contribuição da pesquisa é relacionada sobre evolução e sustentabilidade da arquitetura de software no contexto de ambiente de produção de software centrado em arquitetura.**

***Palavras-chave*— arquitetura de software; conhecimento arquitetural; processo centrado em arquitetura; RM-ODP.**

***Classificação*— Doutorado**

***Categoria*— Iniciante**

I. INTRODUÇÃO

O processo de produção de software torna-se mais complexo, uma vez que não é exigida apenas a criação de novos sistemas de software que atendam os atributos de qualidade desejados, mas também, permitir a capacidade de evolução dos sistemas de software com intuito de acomodar as futuras mudanças, tanto para contemplar a evolução das estratégias de negócio, como também para contemplar a evolução tecnológica [1], [2], [3], [4]. Os envolvidos no ciclo de vida de um sistema de software, de modo explícito ou implícito, relatam os seus interesses que direcionam aspectos sobre o escopo, funcionalidades, requisitos, características operacionais e estruturais do sistema de software. O arquiteto de software deve tomar decisões com relação a estes interesses de diferentes envolvidos, e que afetam os requisitos e os elementos da arquitetura, e consequentemente, levam a mudanças no projeto arquitetural durante todo o processo de construção e evolução da arquitetura. A arquitetura de software deve ser capaz de capturar muitos aspectos que descrevem o sistema, seus componentes, interconexões e o ambiente; como também, guiar a sua evolução arquitetural a cada modificação ou diferente instanciação em um novo produto de software. Para isso, deve ser capaz de documentar as experiências e as lições aprendidas a cada evolução arquitetural.

Desta forma, um problema ainda muito discutido na literatura e como projetar, representar e gerenciar a arquitetura de software, de tal forma, que o esforço exigido para construção e evolução da arquitetura de software existente seja reduzido em um contexto de constantes adaptações e modificações arquiteturais, de forma que, a memória das decisões arquiteturais a cada evolução da arquitetura não seja perdida. Segundo, Capilla et al. (2016), em sua revisão sistemática sobre gerenciamento do conhecimento arquitetural, os métodos existentes para gerenciamento de decisões arquiteturais[5], [6], [7], [8] não apoiam a evolução da arquitetura e a evolução do conhecimento arquitetural [9].

O objetivo da pesquisa é validar o uso do modelo de correspondências do padrão RM-ODP para permitir a rastreabilidade dos interesses das partes interessadas e as modificações e evoluções geradas nos elementos que descrevem a arquitetura de software nas diferentes visões arquiteturais. A contribuição da pesquisa está relacionada com a evolução e a sustentabilidade da arquitetura de software no contexto de ambiente de produção de software centrado em arquitetura. Para isso, serão propostos mecanismos para a captura, documentação, compartilhamento do conhecimento associado a arquitetura de software e ao histórico de evolução da arquitetura ao longo do processo de desenvolvimento do software, de modo a possibilitar rastreabilidade entre os interesses dos envolvidos e as decisões arquiteturais que modificam a arquitetura de software.

II. Referencial Teórico

A. Arquitetura de Software

Para Perry e Wolf (1992) a arquitetura era definida pela fórmula Arquitetura = {Elementos, Forma, Fundamentação}, ou seja, a arquitetura de software definida como um conjunto de elementos arquiteturais que tem uma forma particular; os elementos seriam os principais constituintes de qualquer arquitetura em termos de componentes e conectores, e assim, as propriedades no funcionais gerariam a forma final da arquitetura, e que, poderia ser representada de diferentes formas, mas com a mesma ou similar funcionalidade; como consequência, a base de fundamentação da arquitetura de software formada pelas escolhas de projeto válidas, a partir das quais, o arquiteto de software se baseia para realizar as suas decisões de projeto e definir a arquitetura. Já segundo a IEEE std. 42010 (2011), a arquitetura é definida como a organização fundamental de um sistema incorporada em seus componentes, seus relacionamentos uns com os outros e com seu ambiente, e bem como os princípios que guiam a sua concepção e evolução [10]. O arquiteto de software, no contexto de processo de desenvolvimento de software, é o papel responsável pela arquitetura do sistema, que pode ser uma pessoa, uma equipe ou uma organização. O conceito de arquitetura de software como um conjunto de decisões arquiteturais foi estabelecido por vários autores na literatura [5], [8], [6], [11], [12], entretanto, alguns destacaram a pouca atenção tinha sido dada para a evolução da arquitetura de software [11], [13], já outros ressaltaram importância das decisões arquiteturais e a negligência sofrida durante todo o ciclo de vida da arquitetura [6], [12], uma vez que, as decisões arquiteturais residem na mente do arquiteto como um conhecimento tácito, que raramente é documentado de uma forma que seja utilizável. Como consequência da falta de documentação e a evaporação deste conhecimento foram apontadas como fatores de grande influência sobre a complexidade e o custo de evolução de sistemas de software, e que afetam também a comunicação entre os envolvidos e prejudica o reúso da arquitetura de software [7].

Segundo Capilla et all. (2016) a área de pesquisa de arquitetura de software tem apresentado uma maturidade acentuada nos últimos 30 anos, que culminou com o estabelecimento do papel do arquiteto de software na prática industrial.

Além disso, a arquitetura de software passou a não ser mais definida apenas em termos puramente técnicos, ou relacionados a estrutura de sistemas e comportamento, com componentes e conectores, visões e outros elementos, também passou a considerar elementos sócio técnicos e a considerar a arquitetura de software sob o ponto de vista dos envolvidos e como eles fundamentam e tomam decisões [9]. Já outros autores focam na capacidade da arquitetura de software e das escolhas de projeto arquitetural resistirem ao longo do tempo, e destacam algumas das tendências e abordagens de pesquisa com relação a evolução [13], [14] e a sustentabilidade [15], [16], [4] da arquitetura de sistemas de software de uso intensivo.

B. RM-ODP e a Representação da Arquitetura de Software

A abstração da arquitetura envolve definir um conjunto de visões relevantes aos interesses e as decisões de projeto que endereçam estes interesses. Segundo Rozanski e Woods (2012), as visões são diferentes formas de se observar um mesmo problema, ou seja, as visões arquiteturais são diferentes formas de se observar a arquitetura de um software, cada uma ressaltando aspectos específicos e relevantes de acordo com o papel do envolvido que está definindo a arquitetura e a fase do processo de desenvolvimento no momento. Já ponto de vista é uma coleção de padrões, modelos e convenções para construir um tipo de visualização, para isso, define as partes interessadas cujas preocupações são refletidas no ponto de vista e nas diretrizes, princípios e modelos de modelos para a construção de seus pontos de vista [17]. O RM-ODP é um modelo de referência em computação, que fornece um framework de coordenação para processamento distribuído aberto, vale ressaltar que, este modelo foi difundido por duas entidades padronizadoras (ISO/IEC e ITU-T)[18]. Para isso, ele suporta distribuição, interconexão, independência de plataforma, tecnologia e portabilidade, em conjunto com um framework de arquitetura corporativa para especificação de sistemas processamento distribuído e aberto. O RM-ODP define cinco pontos de vista diferentes e complementares que auxiliam na definição da arquitetura de software de um sistema computacional complexo, para isso, cada ponto de vista representa uma perspectiva do sistema a partir de um conjunto de envolvidos.

Os pontos de vista do RM-ODP são as seguintes [19], [18]: empresa (os requisitos básicos do sistema considerando o contexto da empresa em que o sistema deverá funcionar); informação (a semântica da informação e a semântica do processamento da informação no sistema que deverá estar constituído de objetos informação); computação (estrutura de processadores de informação distribuídos que interagem através de interfaces específicas); engenharia (preocupa-se em especificar mecanismos, funções e estruturas que viabilizam a comunicação entre objetos do tipo computação distribuída no sistema ODP); e tecnologia (seleção de tecnologia para implementar o sistema). É importante ressaltar que cada ponto

de vista possui diferentes interesses no sistema, diferentes requisitos a partir do sistema e diferentes critérios de avaliação, além disso, contêm diferentes informações, e também, diferentes especificações para o sistema [19]. Desta forma, pode-se perceber que cada ponto de vista possui diferentes interesses de diferentes envolvidos no processo de criação, desenvolvimento e evolução da arquitetura de um sistema de software, ou seja, cada envolvido no ciclo de vida da arquitetura de software possui interesses que são capturados pela linguagem de especificação daquele ponto de vista. Para cada ponto de vista existe uma linguagem que pode ser usada para especificar um sistema a partir daquele ponto de vista. O conceito de modelagem objetos fornece uma base comum para a linguagem de especificao de pontos de vista e torna possível a identificação do relacionamento entre as diferentes especificações e para declaração das correspondências entre os modelos do sistema em diferentes pontos de vista [20].

III. Método de Pesquisa

Este trabalho é classificado no quadrante de Pasteur [21] como produto de uma pesquisa aplicada, e que usa o framework Design Science (DS) descrito por Wieringa (2014), que consiste em investigar e projetar um artefato em um contexto visando melhorar algo nesse contexto, como consequência, a melhoria obtida e fruto da implantação de um tratamento que resolve um problema prático do mundo real. O contexto de pesquisa se divide em contexto social e contexto do conhecimento, sendo que, o contexto social se refere a aplicação do artefato em um contexto e que afeta aos interessados no artefato e também o ambiente em que se manifesta o problema que é tratado pelo uso do artefato [22]. O contexto do problema é o processo de produção e evolução de sistemas de software que operam cada vez mais em um ambiente de disponibilidade contínua e que evoluir em resposta as inevitáveis mudanças nos objetivos e requisitos do sistema. Neste contexto, deve-se conhecer o processo de definição e evolução da arquitetura de software e o processo de tomada de decisão par atender os requisitos arquiteturais que modificam a arquitetura de software. O problema da pesquisa é tratar rastreabilidade entre os interesses dos envolvidos e seus requisitos que promovem modificações dos elementos arquiteturais em diferentes visões a cada decisão arquitetural. Para isso, o framework do Design Science Research propõe duas atividades que devem ser executadas: projetar e investigar [22]. A atividade projetar se relaciona com o ciclo de engenharia que consiste das seguintes fases: investigar o problema, projetar o tratamento, validar o tratamento, implantar o tratamento no mundo real e verificar os resultados da implantação do tratamento. Já a atividade de investigar se relaciona a aplicação de métodos de pesquisa analíticos e métodos de pesquisa empíricos que permitam responder perguntas de conhecimento sobre a estrutura e funcionamento dos artefatos projetados.

IV. Desenvolvimento da Proposta

Esta pesquisa dará continuidade as pesquisas sobre ambiente de produção de software centrados em arquitetura do LTS (Laboratório de Tecnologia de Software) da Escola Politécnica. Para isso, será adotado o modelo de Fábrica de Software desenvolvida pelas pesquisas desenvolvidas pelo GARFSoft (Grupo de Arquitetura e Fábrica de Software) do LTS [23], [24], [25], [26] . Desta forma, o ambiente de produção de software centrado em arquitetura utilizará a arquitetura de referência proposta por Naranjo (2018) que propõe uma arquitetura corporativa de referência de Ambiente Colaborativo de Ensino-Aprendizagem e Produção de Software, que teve como estrutura principal o modelo de referência para processamento aberto e distribuído (RM-ODP), e utilizou como base o histórico da operação da disciplina de Laboratório de Engenharia de Software II do curso de Engenharia de Computação entre os anos 2012 e 2017.

Uma das contribuições deste trabalho é complementar a arquitetura de referência definida por Naranjo (2018) através da definição e especifição dos processos de gerenciamento de decisões arquiteturais [27], [28]. Para a representação da descrição arquitetural será baseada na norma de descrição da arquitetura ISO/IEC IEEE 42010 (2011) [10] e no resultado da comparação das propostas de representação de decisões arquiteturais [5], [29], [8]. Também é proposto um modelo para a rastreabilidade das dependências e relacionamentos entre os interesses, requisitos arquiteturais, decisões arquiteturais e os elementos que descrevem a arquitetura de software nas diferentes visões. Para isso, será desenvolvida uma extensão do modelo para representação das decisões arquiteturais através das contribuições das visões arquiteturais e da especificação de correspondências entre os pontos de vista do RM-ODP [19], [30], [18], [31], [20]. O modelo de correspondências entre pontos devista do RM-ODP é adotado para prover os mecanismos de rastreabilidade das dependências entre os interesses arquiteturais de cada envolvido, as decisões arquiteturais e os elementos que descrevem a arquitetura de software.

O formalismo proposto pelo RM-ODP permite agregar maturidade ao modelo, uma vez que, estabelece o processo de especificação dos modelos de cada visão arquitetural, sendo que, cada visão representa um foco particular sobre o sistema especificado. A cada visão representa pontos de vista a partir de um conjunto de envolvidos no sistema e seus respectivos interesses. O formalismo para a representação conhecimento arquitetural e baseado na notação Unified Model Language (UML) para especificação de sistemas ODP apresentado em ISO/IEC 19793 (2014). Este trabalho de pesquisa considera o esquema de pontos de vista do RM-ODP para a representação das visões da arquitetura de software, uma vez que é um padro aderente a computao distribuída e aberta, o que o torna mais abrangente, e por estar bastante amadurecido, tanto na comunidade acadêmica quanto em aplicações no mercado. Além disso, propicia a linguagem de especificação de correspondências entre as visões arquiteturais, o que possibilita o mapeamento das correspondências entre os elementos da documentação arquitetural, e os interesses dos envolvidos, e como novos interesses ou mudanças podem impactar na arquitetura. Para isso, foi formulada a seguinte hipótese de pesquisa:

Hipótese da Pesquisa: O uso do modelo de correspondências entre as visões do padrão RM-ODP possibilita a rastreabilidade entre os interesses dos envolvidos, as decisões arquiteturais e os diferentes elementos da representação da arquitetura a cada evolução da arquitetura de software.

V. Resultados Esperados

A adoção de ambiente de produção de software centrados em arquitetura e o uso de métodos, técnicas e ferramentas de gerenciamento de decisão arquitetural podem contribuir para alcançar as metas de produção de software com mais qualidade, produtividade, custos mais baixos e com maior interoperabilidade, através de apoiar os mecanismos de suporte ao compartilhamento, difusão e entendimento deste conhecimento associado ao processo de construção e evolução de uma arquitetura de software.Para isso, o desenvolvimento desta pesquisa espera contribuir com a melhoria da qualidade de sistemas software de uso intensivo, através de ambientes de produção de software, que incorporem processos, práticas e métodos para produzir arquiteturas de software mais sustentáveis durante todo o ciclo de vida de desenvolvimento de software. Também espera-se contribuir com a área de conhecimento de gerenciamento de conhecimento arquitetural através de um modelo e uma ferramenta para permitir a rastreabilidade entre interesses, requisitos, decisões de projeto e os elementos que descrevem a arquitetura.

References

[1] WOODS, E. Architecting in the gaps: A metaphor for architecture work. *IEEE Software*, v. 32, n. 4, p. 33–35, July 2015. ISSN 0740-7459.

[2] ERDER, M.; PUREUR, P. What's the architect's role in an agile, cloud-centric world? *IEEE Software*, v. 33, n. 5, p. 30–33, Sept 2016. ISSN 0740-7459.

[3] HOHPE, G. et al. The software architect's role in the digital age. *IEEE Software*, v. 33, n. 6, p. 30–39, Nov 2016. ISSN 0740-7459.

[4] VENTERS, C. C. et al. Software sustainability: Research and practice from a software architecture viewpoint. *Journal of Systems and Software*, v. 138, p. 174 – 188, 2018. ISSN 0164-1212. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0164121217303072>.

[5] JANSEN, A.; AVGERIOU, P.; VEN, J. S. van der. Enriching software architecture documentation. *Journal of Systems and Software*, v. 82, n. 8, p. 1232 – 1248, 2009. ISSN 0164-1212. SI: Architectural Decisions and Rationale. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0164121209001046>.

[6] KRUCHTEN, P.; CAPILLA, R.; DUEAS, J. C. The decision view's role in software architecture practice. *IEEE Software*, v. 26, n. 2, p. 36–42, March 2009. ISSN 0740-7459.

[7] CHE, M. An approach to documenting and evolving architectural design decisions. In: *Proceedings of the 2013 International Conference on Software Engineering*. Piscataway, NJ, USA: IEEE Press, 2013. (ICSE '13), p. 1373–1376. ISBN 978-1-4673-3076-3. Disponível em: <http://dl.acm.org/citation.cfm?id=2486788.2487009>.

[8] ZIMMERMANN, O. et al. Architectural decision guidance across projects - problem space modeling, decision backlog management and cloud computing knowledge. In: *2015 12th Working IEEE/IFIP Conference on Software Architecture*. [S.l.: s.n.], 2015. p. 85–94.

[9] CAPILLA, R. et al. 10 years of software architecture knowledge management: Practice and future. *Journal of Systems and Software*, Elsevier, v. 116, p. 191–205, 2016.

[10] ISO, M. *Systems and software engineering–architecture description*. [S.l.], 2011.

[11] BOSCH, J. Software architecture: The next step. In: OQUENDO, F.; WARBOYS, B. C.; MORRISON, R. (Ed.). *Software Architecture*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004. p. 194–199. ISBN 978-3-540-24769-2.

[12] KÖNEMANN, P.; ZIMMERMANN, O. Linking design decisions to design models in model-based software development. In: BABAR, M. A.; GORTON, I. (Ed.). *Software Architecture*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. p. 246–262. ISBN 978-3-642-15114-9.

[13] BREIVOLD, H. P.; CRNKOVIC, I.; LARSSON, M. A systematic review of software architecture evolution research. *Information and Software Technology*, v. 54, n. 1, p. 16 – 40, 2012. ISSN 0950-5849. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0950584911001376>.

[14] BARNES, J. M.; GARLAN, D.; SCHMERL, B. Evolution styles: foundations and models for software architecture evolution. *Software & Systems Modeling*, v. 13, n. 2, p. 649–678, May 2014. ISSN 1619-1374. Disponível em: <https://doi.org/10.1007/s10270-012-0301-9>.

[15] BECKER, C. et al. Sustainability design and software: The karlskrona manifesto. In: *Proceedings of the 37th International Conference on Software Engineering - Volume 2*. Piscataway, NJ, USA: IEEE Press, 2015. (ICSE '15), p. 467–476. Disponível em: <http://dl.acm.org/citation.cfm?id=2819009.2819082>.

[16] LAGO, P. et al. Framing sustainability as a property of software quality. *Commun. ACM*, ACM, New York, NY, USA, v. 58, n. 10, p. 70–78, set. 2015. ISSN 0001-0782. Disponível em: <http://doi.acm.org/10.1145/2714560>.

[17] ROZANSKI, N.; WOODS, E. *Software systems architecture: working with stakeholders using viewpoints and perspectives*. [S.l.]: Addison-Wesley, 2012.

[18] LININGTON, P. F. et al. *Building enterprise systems with ODP: an introduction to open distributed processing*. [S.l.]: Chapman and Hall/CRC, 2011.

[19] PUTMAN, J. R.; BARRY, W. *Open distribution software architecture using RM-ODP*. [S.l.]: Prentice Hall PTR, 2000.

[20] REC, I. X. 906— iso/iec 19793. *Information technology-Open distributed processingUse of UML for ODP systems specifications. Final Committee Draft. Geneva, Switzerland*, 2014.

[21] STOKES, D. E. *O quadrante de Pasteur: a ciência básica ea inovação tecnológica*. [S.l.]: Unicamp, 2005.

[22] WIERINGA, R. J. *Design science methodology for information systems and software engineering*. [S.l.]: Springer, 2014.

[23] BORSOI, B. T.; BECERRA, J. L. A method to define an object oriented software process architecture. In: *2008 19th Australian Software Engineering Conference(ASWEC)*. [s.n.], 2008. v. 00, p. 650–655. ISSN 1530-0803. Disponível em: <doi.ieeecomputersociety.org/10.1109/ASWEC.2008.20>.

[24] BORSOI, B. *Arquitetura de processo aplicada na integração de fábricas de software*. — Escola Politcnica, Universidade de So Paulo, Brasil, 2008.

[25] PESANTES, M.; BECERRA, J. L. R.; LEMUS, C. A method to design a software process architecture in a multimodel environment: An overview. In: *Agile Estimation Techniques and Innovative Approaches to Software Process Improvement*. [S.l.]: IGI Global, 2014. p. 219–242.

[26] NARANJO, J. F. R. *Arquitetura de referÍncia para um ambiente colaborativo de ensino-aprendizagem e produo de software utilizado na graduao de engenharia de computao(Exame de Qualificao)*. Dissertação (Mestrado) — Escola Politcnica, Universidade de So Paulo, Brasil, 2018.

[27] BABAR, M. A. et al. *Software architecture knowledge management*. [S.l.]: Springer, 2009.

[28] MARTIN, J. N. Overview of an emerging standard on architecture processesiso/iec/ieee 42020. In: IEEE. *Systems Conference (SysCon), 2018 Annual IEEE International*. [S.l.], 2018. p. 1–8.

[29] JANSEN, A.; BOSCH, J.; AVGERIOU, P. Documenting after the fact: Recovering architectural design decisions. *Journal of Systems and Software*, v. 81, n. 4, p. 536 – 557, 2008. ISSN 0164-1212. Selected papers from the 10th Conference on Software Maintenance and Reengineering (CSMR 2006). Disponível em: <http://www.sciencedirect.com/science/article/pii/S016412120700194X>.

[30] LININGTON, P. F. Black cats and coloured birds what do viewpoint correspondences do? In: *2007 Eleventh International IEEE EDOC Conference Workshop*. [S.l.: s.n.], 2007. p. 239–246.

[31] JAN, J. I.; ROMERO, J. R.; VALLECILLO, A. Realizing correspondences in multi-viewpoint specifications. In: *2009 IEEE International Enterprise Distributed Object Computing Conference(EDOC)*. [s.n.], 2009. v. 00, p. 163–172. ISSN 1541-7719. Disponível em: <doi.ieeecomputersociety.org/10.1109/EDOC.2009.23>.

COMUNICAÇÕES DE PUBLICAÇÃO

AgronomoBot: a Smart Answering Chatbot Applied to Agricultural Sensor Networks

MOSTAÇO, G. M.*; SOUZA, Í. R. C.†; CAMPOS, L. B.†; CUGNASCA, C. E.*
*Department of Computer Engineering and Digital Systems – Escola Politécnica da Universidade de São Paulo (USP)
São Paulo, Brazil
†Coordination of Information Systems – Instituto Federal de Educação, Ciência e Tecnologia da Bahia (IFBA)
Vitória da Conquista, Bahia, Brazil
E-mail: gmostaco@usp.br

***Abstract*—Mobile devices advanced adoption has fostered the creation of various messaging applications providing convenience and practicality in general communication. In this sense, new technologies arise bringing automatic, continuous and intelligent features for communication through messaging applications by using web robots, also called Chatbots. Those are computer programs that simulate a real conversation between humans to answer questions or do tasks, giving the impression that the person is talking to someone else and not with a computer program. For agricultural purposes, it is important that the data about field conditions, such as air and soil temperature, air relative humidity, soil moisture, rainfall, wind speed and other relevant variables, be rapid and easily available for use by farm management systems, by specialists, or the farmer itself in decision-making processes. AgronomoBot was developed focused on the search and display of data acquired from a Wireless Sensor Network deployed on a vineyard. It is based on Telegram Bot API and is able to access information collected by ekō field sensors, bringing it back to a user through interaction over the Telegram application. The IBM Watson cognition services platform was also used for improving the user experience by enabling the use of natural language during the conversation experience, providing intention detection. Further developments are planned for AgronomoBot, such as the expansion to other messaging platforms, the implementation of speech communication capacity, image classification and continuous data analysis. It is hoped that with analytical capacity over the mass of available data, it becomes possible to work towards the prevention of harmful situations to agricultural productions, early detection of diseases in crops, energy and water waste reduction, and advanced management capabilities for the farmer.**

***Keywords*— Chatbot; Wireless Sensor Networks; Internet of Things; Artificial Intelligence; Watson; Telegram.**

***Classification*— Conference publishing communication: 14th International Conference on Precision Agriculture, June-2018, Montreal-Quebec-Canada [1]**

ACKNOWLEDGEMENTS

The authors want to thank The National Council for Scientific and Technological Development – CNPq and the University of São Paulo for the financial and institutional support to this research .

REFERENCE

[1] G. M. Mostaço, Í. R. C. de Souza, L. B. Campos, and C. E. Cugnasca, "AgronomoBot: a smart answering Chatbot applied to agricultural sensor networks," in *14th International Conference on Precision Agriculture (ICPA)*, (online), Ed. Monticello, IL: International Society of Precision Agriculture, 2018, p. 13.

Sentiment analysis of social network data for cold-start relief in recommender systems

CONTRATRES, F. G.*; ALVES-SOUZA, S. N.*; FILGUEIRAS, L. V. L.*; DESOUZA, L.S.†;
*Universidade de So Paulo - Escola Politcnica, So Paulo, Brazil
†Faculdade de Tecnologia, So Paulo, Brazil
E-mail: felipe.contratres@gmail.com

***Abstract*—Recommender systems have been used in e-commerce to increase conversion due to matching product offer and consumer preferences. Cold-start is the situation of a new user about whom there is no information to make suitable recommendations. Texts published by the user in social networks are a good source of information to reduce the cold-start issue. However, the valence of the emotion in a text must be considered in the recommendation so that no product is recommended based on a negative opinion. This paper proposes a recommendation process that includes sentiment analysis to textual data extracted from Facebook and Twitter and present results of an experiment in which this algorithm is used to reduce the cold-start issue.**

***Keywords*— Social Network; Cold-Start; Recommender Systems; Sentimental Analysis, Social Media**

***Classification*— Article publishing communication**

REFERENCE

[1] Contratres F.G., Alves-Souza S.N., Filgueiras L.V.L., DeSouza L.S. (2018) Sentiment Analysis of Social Network Data for Cold-Start Relief in Recommender Systems. In: Rocha ., Adeli H., Reis L., Costanzo S. (eds) Trends and Advances in Information Systems and Technologies. WorldCIST'18 2018. Advances in Intelligent Systems and Computing, vol 746. Springer, Cham

Fuzzy Logic in Software Defined PON

Utilização da Lógica Fuzzy em Redes PON Definidas por Software

TOMBI, R. G.; HERNÁNDEZ, M. P.; SILVEIRA, R. M.
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica Universidade de São Paulo (USP)
ricardo.tombi@usp.br, {mhernandez, regina}@larc.usp.br

***Abstract*—Passive optical networks (PON) have been increasingly used by telecom operators as access networks and have well-defined resource control mechanisms for downstream and upstream traffic. However, the integration of other technologies such as Fuzzy logic and software defined networks (SDN) can be used as an alternative to optimize or increase the performance of these access networks. This work demonstrates the use of Fuzzy logic for resource allocation in PON networks, and presents how it can be flexible and simple implementation in conjunction with an SDN architecture considering different types of traffic generated by IoT (Internet of Things), voice and video applications, which have specific needs. The results obtained prove the feasibility of Fuzzy logic to subsidize the control of resource allocation, guaranteeing the quality of services in PON.**

***Keywords*— PON, Software Defined Networks, Fuzzy Logic.**

***Resumo*—As redes ópticas passivas (PON) são cada vez mais utilizadas pelas operadoras de telecomunicações como redes de acesso, e possuem mecanismos de controle de recursos bem definidos para o tráfego *downstream* e *upstream*. Entretanto, a integração de outras tecnologias como a lógica Fuzzy e as redes definidas por software (SDN – *Software Defined Network*), podem ser utilizadas como alternativa para otimizar ou aumentar o desempenho destas redes de acesso. Este trabalho demonstra a utilização da lógica Fuzzy para alocação de recursos em redes PON, e apresenta como a mesma pode ser flexível e de simples implementação em conjunto com uma arquitetura SDN considerando tipos distintos de tráfego gerados por aplicações de IoT (*Internet of Things*), voz e vídeo, que apresentam necessidades específicas. Os resultados obtidos comprovam a viabilidade da lógica Fuzzy para subsidiar o controle de alocação de recursos, garantindo a qualidade de serviços em redes PON.**

***Palavras-chave*— PON, Redes Definidas por Software, Lógica Fuzzy.**

***Classificação*— Comunicação de Publicação**

PUBLICATION

[1] TOMBI, R. G.; HERNÁNDEZ, M. P.; SILVEIRA, R. M. Utilização da Lógica Fuzzy em Redes PON Definidas por Software. *XXXVI Simpósio Brasileiro de Telecomnicações e Processamento de Sinais,* Campina Grande, Set, 2018.

Social Network Data to Alleviate Cold-Start in Recommender System: A Systematic Review

GONZALEZ CAMACHO,L.A.*; ALVES-SOUZA, S.N.*
*Laboratrio de Tecnologia de Software-LTS, Departamento de Engenharia de Computação e Sistemas Digitais
E-mail: alejandragc@usp.br, ssouza@usp.br

***Abstract*—Recommender Systems are currently highly relevant for helping users deal with the information overload they suffer from the large volume of data on the web, and automatically suggest the most appropriate items that meet users needs. However, in cases in which a user is new to Recommender System, the system cannot recommend items that are relevant to her/him because of lack of previous information about the user and/or the user-item rating history that helps to determine the users preferences. This problem is known as cold-start, which remains open because it does not have a final solution. Social networks have been employed as a good source of information to determine users preferences to mitigate the cold-start problem. This paper presents the results of a Systematic Literature Review on Collaborative Filtering-based Recommender System that uses social network data to mitigate the cold-start problem. This Systematic Literature Review compiled the papers published between 2011-2017, to select the most recent studies in the area. Each selected paper was evaluated and classified according to the depth which social networks used to mitigate the cold-start problem. The final results show that there are several publications that use the information of the social networks within the Recommender System; however, few research papers currently use this data to mitigate the cold-start problem.**

***Keywords*— Cold start; Social Network; Collaborative Filtering; Recommender System; Systematic Literature Review**

***Classification*— Article publishing communication**

REFERENCE

[1] GONZALEZ CAMACHO,L.A; ALVES-SOUZA, S.N; Social Network data to alleviate cold-start in recommender system: A systematic review. *Information Processing & Management* (JCR=3,4). v. 54, n. 4, p.529-544, Jul, 2018.

Control of Gene Regulatory Networks Basin of Attractions with Batch Reinforcement Learning

NISHIDA, C. E. H.*; COSTA, A. H. R.*; BIANCHI, R. A. C.†
*Escola Politécnica - Universidade de São Paulo
†Departamento de Engenharia Elétrica Centro Universitário FEI
E-mail: {cyntiaeico,anna.reali}@usp.br, rbianchi@fei.edu.br

***Abstract*—Basin of attraction contains biological functions and channels cell behavior, so when a gene network is in an unhealthy basin it may cause diseases. Control techniques can support the design of therapies that promote the transition of a biological system from diseased to healthier basins. Most control methods first infer a gene network and then derive a control strategy to avoid diseased states. However, this approach is limited to few genes and may cause other diseases, as the biological side of the problem is not considered. While changing between basins may change a diseased biological function for a healthier one, state avoidance can change functions in an unexpected way. We propose to extend a batch reinforcement learning method FQISarsa, to change basin of attractions in a partial observable network. Using a batch reinforcement learning technique avoids the most time consuming phases that are the inference and control of the gene network. Results demonstrate that our method, BOAFQI-Sarsa, is more effective than previous studies that do not consider basins in their computations.**

***Keywords*— batch reinforcement learning; gene networks**

***Classification*— Article publishing communication**

REFERENCE

[1] NISHIDA, C. E. H.; COSTA, A. H. R. ; BIANCHI, R. A. C. (in press). Control of Gene Regulatory Networks Basin of Attractions with Batch Reinforcement Learning. In: Brazilian Conference on Intelligent Systems, 2018, São Paulo.

Adaptivity: One phenomenon, multiple perspectives of study

CAYA, R.*; NETO, J. J.*
*Adaptive Technology Laboratory, Department of Electrical and Computer Engineering Polytechnic School, University of So Paulo
E-mail: rosalia.caya@usp.br, joao.jose@poli.usp.br

***Abstract*—This article studies adaptivity as a general phenomenon, a subject of matter, permeable to different perspective within the research areas. From simple and general definitions grounded in Biology and Psychology to sophisticated and particular definitions within Computer technology areas, such as Computer Science, Information Technology, and Software Engineering, this work focus in retrieving the core features that characterize adaptivity, its needs, the different connected areas and the characteristic problems it is suited to solve. We present a proposal for the holistic characterization of adaptive behavior that contributes in the establishment of a framework to share scientific knowledge regarding specification, representation, modeling, design and implementation of adaptive behavior in the technological arena.**

***Keywords*— Adaptivity; self-* systems; complexity; cybernetics; autonomic computing.**

***Classification*— Article publishing communication**

REFERENCES

[1] CAYA, R.; NETO, J. J. Adaptivity: One phenomenon, multiple perspectives of study. In: *Memrias do XII Workshop de Tecnologia Adaptativa - WTA 2018*. EPUSP, 2018. p. 37–47. ISBN 978-85-86686-98-6. Disponível em: <http://lta.poli.usp.br/lta/publicacoes/artigos/2018/caya-e-neto-2018-adaptivity-one-phenomenon-multiple-perspectives-of-study/view>.

A Bibliometric Review about Adaptivity

CAYA, R.*; NETO, J. J.*
*Adaptive Technology Laboratory, Department of Electrical and Computer Engineering Polytechnic School, University of Sao Paulo
E-mail: rosalia.caya@usp.br, joao.jose@poli.usp.br

***Abstract*—The last decades adaptivity has become an increasingly popular feature within both the commercial and academic context, with publications related to this subject appearing more frequently. This article reviews the research on adaptivity in the two contexts, by conducting a bibliometric review of the available research literature related to the subject. By using bibliometric indexes the results found here can be replicated, complemented and extended in a systematic way, incrementing its utility. The study examines the growth pattern of research in adaptivity, and retrieves some: its top areas; types of publications; and contributing countries and organizations. The review also revealed the value for some of the parameters needed to develop more specialized analysis in adaptivity, such as: scope, timespan, search space and databases. Finally, we propose several analysis to be performed in future works to complement the previous results. This work is, to our knowledge, the first bibliometric review conducted for the subject matter of adaptive behavior.**

***Keywords*— adaptivity; bibliometric study.**

***Classification*— Article publishing communication**

REFERENCES

[1] CAYA, R.; NETO, J. J. A bibliometric review about adaptivity. *Procedia Computer Science*, v. 130, p. 1114 – 1119, 2018. ISSN 1877-0509. The 9th International Conference on Ambient Systems, Networks and Technologies (ANT 2018) / The 8th International Conference on Sustainable Energy Information Technology (SEIT-2018) / Affiliated Workshops. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1877050918305295>.

Designing a reference architecture for a collaborative software production and learning environment

NARANJO, J. F. R.; ROSSI, A. C.; ALVEZ-SOUZA, S. N., BECERRA, J. L. R.
*Laboratório de Tecnologia de Software - Universidade de São Paulo
{felipe.restrepo, ana.rossi, ssouza, Jorge.becerra}@usp.br,

***Abstract*—Software engineering is both a body of knowledge and a competence, thus its teaching requires students to get involve in actual software development. For this purpose, a teaching-learning controlled software production environment can be designed. Typically, this environment has been designed as a learning software factory whit focus on the processes, which may lead to a narrowed understanding of the information systems technology required for its successful implementation, operation, and management. We present an ongoing design science research aimed to improve the design of modern Collabo-rative Software Production Teaching-Learning Environments (CSPLE) by using a set of models to describe not only its pro-cesses, but also the information generated by the processes, the software applications used to support the processes execution and the technological infrastructure required to run the applications. These models describing a CSPLE correspond to a set of archi-tectural views compounding an enterprise architecture that can be used as a reference to design specific CSPLE in the context of a practical software engineering course. A preliminary result presented in this paper is a method to design an Enterprise Reference Architecture (ERA) for a CSPLE. The proposed method is also applied giving as empirical highlights about the design of an ERA for a CSPLE.**

***Keywords*— enterprise reference architecture; learning software factory; design science research; RM-ODP.**
***Classification*— Article publishing communication**

***Resumo*—A engenharia de software é tanto um corpo de conhecimento quanto uma competência, por isso o seu ensino exige que os alunos se envolvam em desenvolvimento de software real. Com esse propósito, projetam-se ambientes controlados de ensino-aprendizagem de produção de software. Normalmente, esses ambientes têm sido projetados como fábricas de software de ensino e com foco nos processos, o que pode levar a um entendimento limitado dos sistemas e da tecnologia de informação requerida para sua adequada implementação, operação e gestão. Esta pesquisa em andamento tem como objetivo melhorar o projeto de ambientes colaborativos de ensino-aprendizagem de produção de software (CSPLE) modernos. A proposta é utilizar um conjunto de modelos para descrever não apenas os processos do CSPLE, mas também as informações geradas pelos seus processos, as aplicações de software usados para suportar a execução desses processos e a infraestrutura tecnológica necessária para executar essas aplicações. Esses modelos que descrevem um CSPLE correspondem a um conjunto de visões arquiteturais que compõem uma arquitetura corporativa que pode ser usada como referência para projetar CSPLE específicos no contexto de um curso prático de engenharia de software. O resultado preliminar aqui apresentado é um método para projetar uma arquitetura corporativa de referência (ERA) para um CSPLE. O método proposto é aplicado e se apresentam destaques empíricos sobre o projeto de um ERA para um CSPLE.**

***Palavras-chave*— arquitetura corporativa de referência; RM-ODP; fábrica de software de aprendizagem; ciência de projeto.**
***Classificação*— Comunicação de publicação.**

REFERENCES

[1] NARANJO, J. F. R.; ROSSI, A. C.; ALVEZ-SOUZA, S. N., BECERRA, J. L. R. Designing a reference architecture for a collaborative software production and learning environment. *XIII Conferência Latino-americana de Tecnologias de Aprendizagem LACLO,* Oct, 2018

Personal Data Transparency Analysis in Data Privacy Policies

Análise da Transparência de Dados Pessoais em Políticas de Privacidade de Dados

COLETI, T. A.[*]; MORANDINI, M. [†]; FILGUEIRAS, L. V. L.[*]; CORREA, P. L. P. [*]
[*] Departamento de Engenharia de Computação e Sistemas Digitais da Escola Politécnica da Universidade de São Paulo.
[†]Escola de Artes, Ciências e Humanidades da Universidade de São Paulo (EACH-USP)
{thiagocoleti, m.morandini, lfilguei@usp.br, pedro.correa}@usp.br

***Abstract* — This paper presents a survey-based evaluation of Personal Data Transparency in well-known, widely-used software applications. Transparency aims to inform people on how their personal data are collected, used and disclosed, so that they can have not only knowledge about these processes but also agency in them. The survey was answered by regular users, after they had read the Data Privacy policies of each application. Subjects answered a questionnaire with 8 questions about features intended to support transparency. Results reveal that, although a few transparency features were considered appropriated, some still require improvements, mainly those related to computational infrastructure.**

Keywords— Personal Data Transparency, Data Privacy Policies; Human-Data Interaction.

***Resumo*— Este artigo apresenta uma avaliação de Transparência de Dados Pessoais realizada em aplicações conhecidas e utilizadas por um grande número de usuários. Transparência busca proporcionar informações de como dados pessoais são coletados, utilizados e compartilhados entre sistemas e assim permitir que o indivíduo produtor tenha conhecimento e possa agir dentro deste processo. A pesquisa foi realizada com usuários comuns que avaliaram as políticas de privacidade e termos de uso das aplicações e responderam a um questionário com 8 questões sobre aspectos que deveriam fornecer transparência. Os resultados mostraram que alguns elementos foram considerados transparentes, mas outros, normalmente relacionados à infraestrutura computacional, ainda requerem melhorias.**

Palavras-chave— *Transparência de Dados Pessoais; Políticas de Privacidade e Segurança; Interação-Humano Dados*.
***Classificação*— Comunicação de Publicação**

REFERENCE

[1] COLETI, Thiago Adriano et al. Análise da Transparência de Dados Pessoais em Políticas de Privacidade de Dados. **Anais do Workshop de Aspectos da Interação Humano-Computador na Web Social**, [S.l.], v. 9, p. 025 - 036, sep. 2018. Disponível em: <http://portaldeconteudo.sbc.org.br/index.php/waihcws/article/view/3893>. Qualis Capes: B2

Combining metrics for route selection in SDWSN: static and dynamic approaches evaluation

Oliveira, D. A. G.*; Margi, C. B.*
*Escola Politécnica - Universidade de São Paulo
E-mail: doriedson@usp.br, cintia@usp.br

***Abstract*—The Software Defined Networking paradigm has been applied to Wireless Sensor Networks (WSN) aiming to provide flexibility, enable resource sharing and reuse, and improve management. Routing protocol plays an important role in energy consumption given that the radio is the most power hungry component. Previous works show that using link quality as a metric usually decreases latency while using energy might balance the network energy consumption, thus increasing the network lifetime. We here apply and evaluate energy-aware route selection to Software Defined WSNs through dynamic and static combination of link quality and energy metrics. Dynamic combination is achieved using Fuzzy logic methods. Simulation results show that using energy as a metric achieves the best network lifetime and good energy consumption. Route selection using dynamic combination at CENTROID SCENARIO as a metric shows the best results for packet delivery rate, end-to-end delay and distribution of the nodes energy consumption among the network, where neighbors within the same hop count from the sink or controller have uniform energy consumption, besides a good network lifetime.**

***Keywords*— software defined wireless sensor networking; fuzzy logic; routing metrics.**

***Classification*— Article publishing communication**

REFERENCE

[1] Oliveira, D. A. G; Margi, C. B. Paper title. *Combining metrics for route selection in SDWSN: static and dynamic approaches evaluation* (under submission). IEEE Latin-American Conference on Communications, Nov, 2018.

Energy and performance costs evaluation for BLE mesh links

SILVA, H. C.*; MARGI, C. B.*
*Laboratório de Arquitetura de Redes e Computadores - Escola Politécnica da Universidade de São Paulo
E-mail: {henrique.c.s,cintia}@usp.br

***Abstract*—Bluetooth Low Energy (BLE for short) is among the favorites to become a de facto standard in the context of the Internet of Things (IoT). However, its main challenge is the lack of standards for efficient mesh networking. Furthermore the literature lacks works analyzing energy consumption trade-offs for BLE mesh networks. We address this issue by experimentally evaluating three minimum topologies for linking separate BLE star networks. We aim to determine a lower boundary in terms of energy and performance costs using the metrics of energy consumption, delivery rate, and goodput. We perform our experiments using a testbed comprised of TI CC1350 nodes running Contiki OS. Our results show that, for this lower boundary, there is a trade-off between energy cost and delivery rate in intense network traffic scenarios.**

***Keywords*— Internet of Things; Mesh networks; Bluetooth Low Energy (BLE).**

***Classification*— Article publishing communication**

REFERENCE

[1] SILVA, Henrique Carvalho; MARGI, Cíntia Borges. Energy and performance costs evaluation for BLE mesh links. *Anais do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, [S.l.], v. 36, may 2018. ISSN 2177-9384. Disponível em: ¡http://ojs.sbc.org.br/index.php/sbrc/article/view/2452¿. Acesso em: 17 oct. 2018.