Projeto de Formatura – 2023

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia de Computação

Tema: **Machine Learning aplicada a segurança em Internet das Coisas: detectando anomalias na comunicação e operação**

Motivação

- Utilização de redes de dispositivos de Internet das Coisas na sociedade e indústria: Segurança é requisito crítico.
- Implementação de Sistema de Detecção de Intrusão utilizando as métricas de rede e de operação dos dispositivos.
- Capacidade de detectar ataques "Day-Zero" utilizando aprendizado supervisionado.

Método

- Coleta e tratamento de dados de rede e operação dos dispositivos
- Modelo classificador binário para categorizar a ocorrência de ataque.
- Teste do modelo por meio de validação treino-teste e detecção de ataques “Out of Distribution”

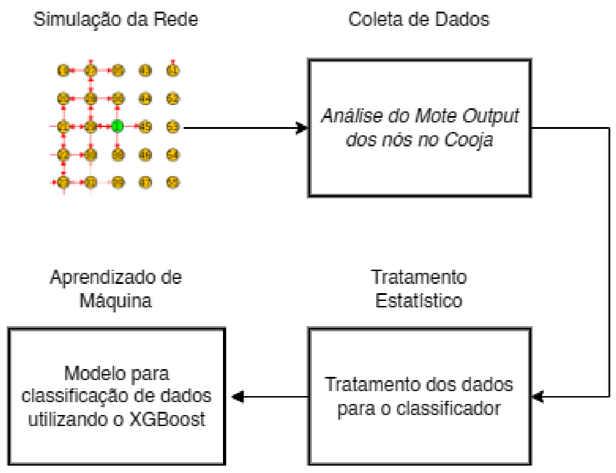

Figura 1: Fluxo do desenvolvimento da pesquisa conforme o método definido. Na figura são apresentados quatro etapas: Simulação da Rede, Coleta de Dados, Tratamento Estatístico e Aprendizado de Máquina.

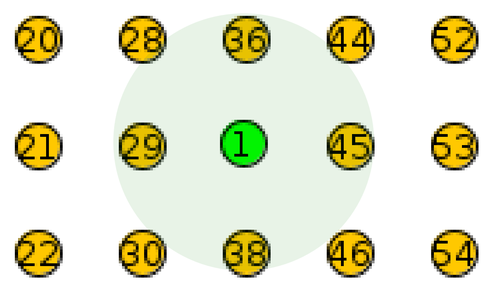

Figura 2: Exemplo de topologia de rede do simulador Contiki Cooja. A figura apresenta a o nó servidor (nó 1, em verde) e os nós clientes (nós em laranja). O alcance de comunicação entre nós é representado pelo círculo em verde claro.

Coleta de Dados

- Utilização do simulador Contiki Cooja: Emulação de dispositivos IoT.
- Implementação dos ataques Flooding, Black e Grey hole. WTICG SBSeg 23.
- Coleta de dados pela interface de Mote Output do servidor.

Figura 3: Repositório do artigo apresentado no WITCG do SBSeg 23 no Github.

Tratamento Estatístico

- Janelamento dos dados utilizando uma fila (”First-In First-Out”).
- Cálculo das médias e desvios padrões dos dados janelados.
- Criação de dataset para o modelo de aprendizagem supervisionada.

Aprendizado de Máquina

- Utilização do XGBoost Classifier para a detecção de intrusão.
- Balanceamento dos dados por meio de ponderamento por classificação.
- Cálculo das métricas de avaliação do modelo por meio da matriz de confusão dos resultados.

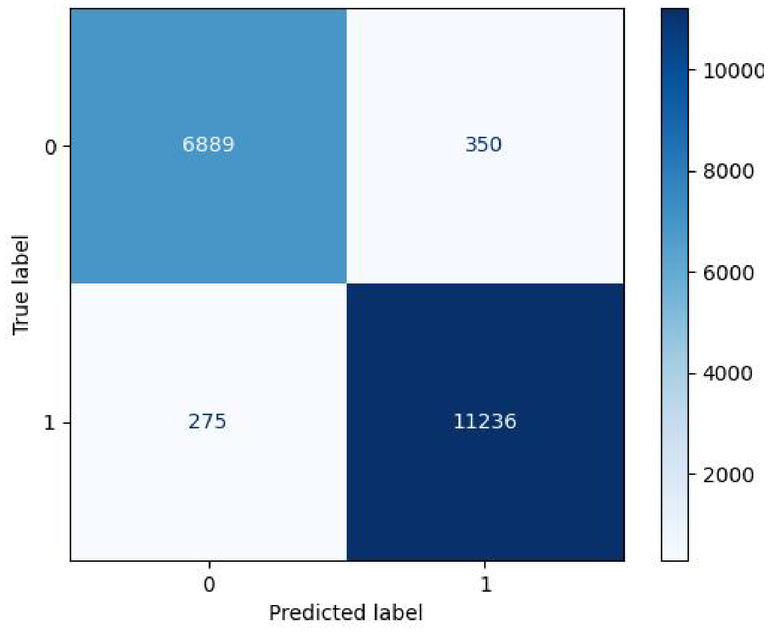

Figura 4: Matriz de confusão do modelo classificador. A figura apresenta o resultado dado pelo classificador e o resultado esperava em uma matriz com os valores em seus eixos.

Resultados

- Sistema capaz de detectar intrusões com acurácia geral de 96%, Com o recall priorizado no sistema.
- Abordagem centralizada se demonstra como uma solução viável no viés de segurança, mas acarreta no aumento da quantidade de pacotes transmitidos na rede.

Figura 5: Repositório do trabalho no Github. Escaneie para poder ver o trabalho em detalhes.

Agradecimentos

< c²d_ centro de ciência de dados >

CAPES

FAPESP

Integrante: Alexandre Marques Carrer

Professor(a) Orientador(a): Profa. Dra. Cíntia Borges Margi

Co-orientador(a): Prof. Dr. Artur Jordão Lima Correia