RENZO ARMANDO DOS SANTOS ABENSUR

DETECÇÃO DE ATAQUES DE BURACO NEGRO E BURACO DE MINHOCA EM REDES DE SENSORES SEM FIO DEFINIDAS POR SOFTWARE

São Paulo
2023

RENZO ARMANDO DOS SANTOS ABENSUR

DETECÇÃO DE ATAQUES DE BURACO NEGRO E BURACO DE MINHOCA EM REDES DE SENSORES SEM FIO DEFINIDAS POR SOFTWARE

Trabalho apresentado à Escola Politécnica da Universidade de São Paulo para obtenção do Título de Engenheiro Eletricista com ênfase em Computação.

São Paulo
2023

RENZO ARMANDO DOS SANTOS ABENSUR

DETECÇÃO DE ATAQUES DE BURACO NEGRO E BURACO DE MINHOCA EM REDES DE SENSORES SEM FIO DEFINIDAS POR SOFTWARE

Trabalho apresentado à Escola Politécnica da Universidade de São Paulo para obtenção do Título de Engenheiro Eletricista com ênfase em Computação.

Orientador:

Profa. Dra. Cíntia Borges Margi

São Paulo
2023

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

PARTE I

INTRODUÇÃO

1 INTRODUÇÃO

1.1 Contextualização

As redes definidas por software (ou *software-defined networking* - SDN) são um conceito de rede que busca deixar mais dinâmico, flexível e escalável as redes tradicionais, revolucionando o atual sistema de redes, a partir da separação entre o plano de controle do plano de dados [1]. A necessidade da tecnologia SDN surgiu num contexto de novas demandas de uso das redes tradicionais, principalmente, nas áreas de, enterprise e ISP network. Dessa forma, a SDN provê uma solução para alta demanda de recursos, manuseio de tráfego de dados e rápida reconfiguração de rede.

No conceito das redes tradicionais o roteamento dos pacotes é dado por um controle pré instalado nos roteadores que englobam o plano de controle e o plano de dados juntos. Por este motivo a administração desses roteadores, geralmente, requerem um grande esforço por parte dos administradores, uma vez que, todos os nós da rede precisam ser atualizados manualmente para que funcionem de forma adequada no controle de transmissão dos pacotes [2]. Dessa forma,com a demanda para a adaptação ao atual cenário de crescimento na diversidade de dispositivos conectados na rede, surge o conceito de redes definidas por software (SDN). Este paradigma promete eliminar as limitações das redes tradicionais, por meio da utilização de uma lógica de controle separada do hardware e do plano de dados e centralizada em um plano de controle remoto.

Como consequência, os roteadores se transformam em dispositivos que não sabem mais como se comunicar com os outros nós da rede de forma autônoma. A função deles torna-se a de redirecionar de forma eficiente o fluxo de dados entre os nós da rede. Já a parte do roteamento, é centralizada no plano de controle, o que evita a necessidade de modificar todos os switches sempre que um novo nó é adicionado à rede ou alguma modificação de roteamento for realizada. Neste contexto as SDN vem ganhando força como uma alternativa viável à diversas aplicações que visam, principalmente, a flexibilidade e escalabilidade da rede.

Dentre as aplicações que se beneficiariam deste novo paradigma de rede, destacam-se as redes de sensores sem fios (RSSF) e internet das coisas (Internet of Things - IoT). Neste tipo de rede a flexibilidade e a eficiência de recursos são de extrema impotância para um funcionamento adequado. Desta forma, com a utilização da SDN, tarefas como a de configurar e reconfigurar novos dispositivos IoT tornariam-se muito mais simples e rápidas. Além disto, por demandarem menos configurações complexas de rede, os recursos dos dispositvos IoT dentro da rede podem ser realocados de forma mais eficientes, o que é de extrema importância para dispostivos que operam com recursos limitados. Portanto, as redes SDN seriam uma solução desejável para este tipo de aplicação.

Contudo, apesar dos diversos benefícios que estas redes podem trazer às RSSF em IoT estas ainda possues diversas vulnerabilidades de segurança que podem ser exploradas e, portanto, devem ser sanadas antes da utilização deste novo paradigma de rede. As SDN por possuírem um plano de controle centralizado e separado do plano de dados adiciona novos desafios de segurança ás redes.

Dessa forma, o foco deste projeto é a verificação de possíveis ataques e possíveis detecção destes ataques nas redes SDNs em RSSF, verificando os riscos deste ataque e o impacto na rede como um todo. O ataque que será explorado foca em utilizar dispositivos com potência de rádio de alcance maior em um do nós da rede de sensores sem fio (RSSF) que utilizam SDN, e verificar as possibilidades de ataques do tipo buracos negros e buracos de minhoca.

1.2 Definição do problema

O problema que está sendo explorado foca na segurança das redes SDN no contexto de redes de sensores sem fio, quando nós da rede com enlaces assimétricos, são modificado para se tornar nós maliciosos e causar ataques do tipo ataques de negação de serviço (*Denial of Service* - DoS) ou buraco de minhoca.

Devido a grande variedade das aplicações existentes em RSSF, os requisitos de segurança da informação, como: autenticidade, integridade, confidencialidade e disponibilidade, são necessários. Por exemplo, em uma RSSF ligadas à área da saúde a confidencialidade e a autenticidade dos dados são de extrema importância para garantir a segurança das informações individuais dos pacientes. Por outro lado, em uma aplicação de RSSF em agricultura a integridade e disponibilidade dos dados na rede são de extrema importância para gerar relatórios adequados de estudo climáticos de uma região. Ape-

sar disso, a implementação destes requisitos de segurança são um desafio no contexto de recusos limitados.

Dessa forma, o projeto explora ataques possíveis de serem realizados em RSSF em específico em enlaces assimétricos, quando um ou mais nós maliciosos com potência de rádio de maior alcance busca afetar o encaminhamento seletivo dos nós da rede.

1.3 Objetivo

O objetivo principal deste trabalho é analisar como enlaces assimétricos em RSSF podem viabilizar novos ataques em redes definidas por software. Para tanto, os ataques serão implementados e simulações de rede realizadas para que seja possível validar e comparar o impacto que a adição de um ou mais nós maliciosos podem causar na rede.

2 FUNDAMENTOS E TRABALHOS RELACIONADOS

Este capítulo é focado em apresentar fundamentos técnicos básicos sobre redes SDN, RSSF/IoT e enlaces assimétricos, que serão importantes para o entendimento e desenvolvimento deste projeto.

2.1 Arquitetura das Software-Defined Networking

Com o interesse de desenvolver uma rede para reduzir os custos de implementação e os custos de operação com serviços de provedores e enterprise e data centers, surgiu a ideia das SDN, com o objetivo de desenvolver uma arquitetura baseada em redes programáveis. A partir deste paradigma as redes SDN se baseiam na separação do plano de controle do plano de dados. Nesta arquitetura os controladores são responsáveis por decidir o roteamento do plano de dados da rede e, consequentemente, os dispositivos da rede possuem apenas a necessidade de realizar o encaminhamento seletivo dos pacotes de acordo com as definições do plano de controle.

Dessa forma, a arquitetura das SDN é dividida em três principais planos: o plano de dados, o plano de controle e o plano de aplicação. O plano de dados tem a função de realizar o "selective forwarding" dos pacotes e é onde os switches se encontram. Já o plano de controle tem a função de controlar toda a lógica da rede, definindo para isso, como os pacotes do plano de dados devem ser configurados e roteados por cada switch. Por fim, o plano de aplicação é onde o usuário interage com os controladores e garante a operação otimizada da rede por meio do controle e monitoramento da rede. Além disso, a arquitetura das SDN separa sua comunicação em 3 módulos externos que interagem com o controlador. Eles são classificados dependentes da direção em que a interação ocorre no sistema, sendo eles divididos em Southbound interface, Northbound interface e East and West interface.

A *Southbound Interface* é o protocolo de comunicação que está relacionada com a

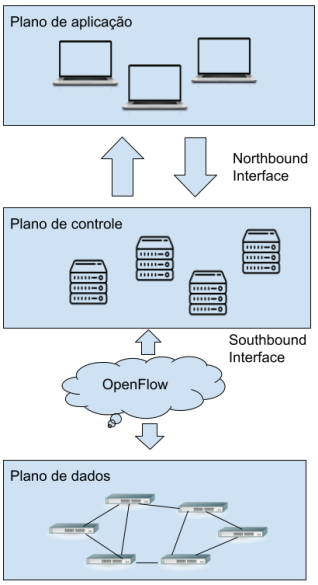

Figura 1: Protocolos em SDN [1]

conexão entre o plano de controle e o plano de dados (switches). O framework deste protocolo mais utilizado, atualmente, é o OpenFlow, que é responsável por instalar o flows nos switches de acordo com o as políticas pré definidas pelos controladores, além de ser responsável por enviar ao controlador informações de estatísticas de roteamento e mudanças na arquitetura do plano de dados.

Já a *Northbound Interface* está relacionada com todas as interações que o usuário tem com o controlador, atualmente ainda não existe um framework padrão nesta interface. Porém, os desafios encontrados para a implementação deste protocolo se baseiam em criar uma forma segura de comunicação entre o usuário e o controlador, assim como gerir as permissões e autorizações e os conflitos entre diferentes aplicações.

Por fim, a *East and West Interface* que, apesar de não estar presente em todas as SDN, está relacionada com o controle de SDNs distribuídas, onde, por exemplo, existe uma ordem hierárquica entre os controladores e um controlador principal fica responsável por gerir diversos controladores "filhos" e responsável pela troca de informações e controle no sistema, além de definir o acesso de cada filho na rede.

2.2 RSSF / IoT

As redes de sensores sem fio (RSSF) são redes compostas por diversos dispositivos microeletrônicos chamados de nós, que utilizam-se de comunicação de rádio sem fio para trocar dados e informações do ambiente entre si e entre outras redes sem fio. A forma

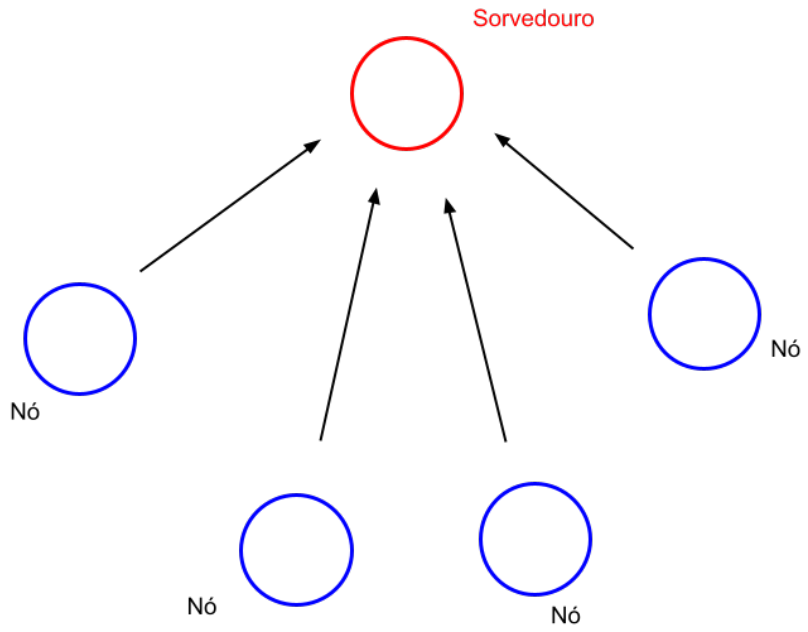

Figura 2: Padrão de comunicação em RSSF

mais comum de implementação de uma RSSF é baseada na comunicação muitos para um onde vários nós “padrão” se comunicam com um nó “principal” chamado de sorvedouro, responsável por coletar e guardar as informações referentes aos nós “padrão”.

Dessa forma, as RSSF são extremamente valiosas pela sua maleabilidade e diversidade de aplicações, elas podem ser utilizadas deste aplicações relacionadas com o monitoramento ambiental, aplicações relacionadas a saúde ou ainda aplicações relacionadas a redes sociais. Contudo, por este tipo de rede ser muito maleável algumas características devem ser consideradas em cada aplicação, tais como consumo de energia ou recursos computacionais, o que dificulta a adoção de um protocolo padrão nesse tipo de rede.

Portanto, apesar das RSSF possuírem alguns padrões de roteamento de pacotes, cada RSSF que é implementada foca em adotar um protocolo específico de implementação, visando melhorar alguma das métricas da rede. Por exemplo, melhorar o uso de energia, ou diminuir a latência ou aumentar a confiabilidade da rede. Sendo assim, a escolha de um protocolo de roteamento padrão para as RSSF é muito dependente da aplicação em que a rede se encontra, o que pode gerar conflitos entre redes em que as aplicações dependam

de métricas diferentes, aumentando a complexidade do desenvolvimento e administração deste tipo de rede.

Dessa forma, as SDN em RSSF surgiram como uma maneira eficiente de conciliar essa complexidade de roteamento, por meio das redes definidas por software.

2.3 IT-SDN

O IT-SDN [8] é uma ferramenta aberta específica para a implementação e experimentação de redes definidas por software (SDN) em redes de sensores sem fio (RSSF). Esta ferramenta utiliza-se de ferramentas do sistema operacional Contiki OS e utiliza-se de três principais protocolos de comunicação: o protocolo *southbound* , o protocolo de descoberta de vizinhos e o protocolo de descoberta de controlador

O protocolo *southbound* é responsável pela comunicação entre o controlador e os nós da rede SDN, para ser realizado o roteamento adequados dos pacotes. Já o protocolo de descoberta de vizinhos é responsável pelo gerenciamento das informações de nós vizinhos da rede. E por fim, o protocolo de descoberta de controlador que é responsável por encontrar o roteamento dos pacotes para alcançar o controlador da rede [6].

Além disso, esta ferramenta utiliza-se de implementação de software no controlador para realizar o roteamento eficiente dos nós na rede. Para isso, o software implementado utiliza-se de algoritmos como o Djikstra para gerar a topologia da rede e tomar decisão de roteamento.

2.4 Enlaces assimétricos

A definição de enlaces assimétricos está relacionada com redes heterogêneas onde os nós utilizam potências de transmissão diferentes para se comunicar entre si [2]. As redes de sensores sem fio dependem de um sinal de rádio limpo, com baixa taxa de ruídos, para decodificar pacotes de forma correta e eficiente, dessa forma, a comunicação sem fio pode se tornar assimétrica quando os nós utilizam potências de rádios diferentes.

Diversos fatores podem transformar enlaces simétricos de uma RSSF em enlaces assimétricos, por exemplo, condições meteorológicas, interferências do meio, antenas não isotrópicas ou dispositivos com diferentes potências de rádio. Além disso, este efeito costuma ser amplificado em redes de comunicação com baixa potência onde os dispositivos são de baixo custo e consequentemente baixa qualidade de transmissão, ou são dispositivos

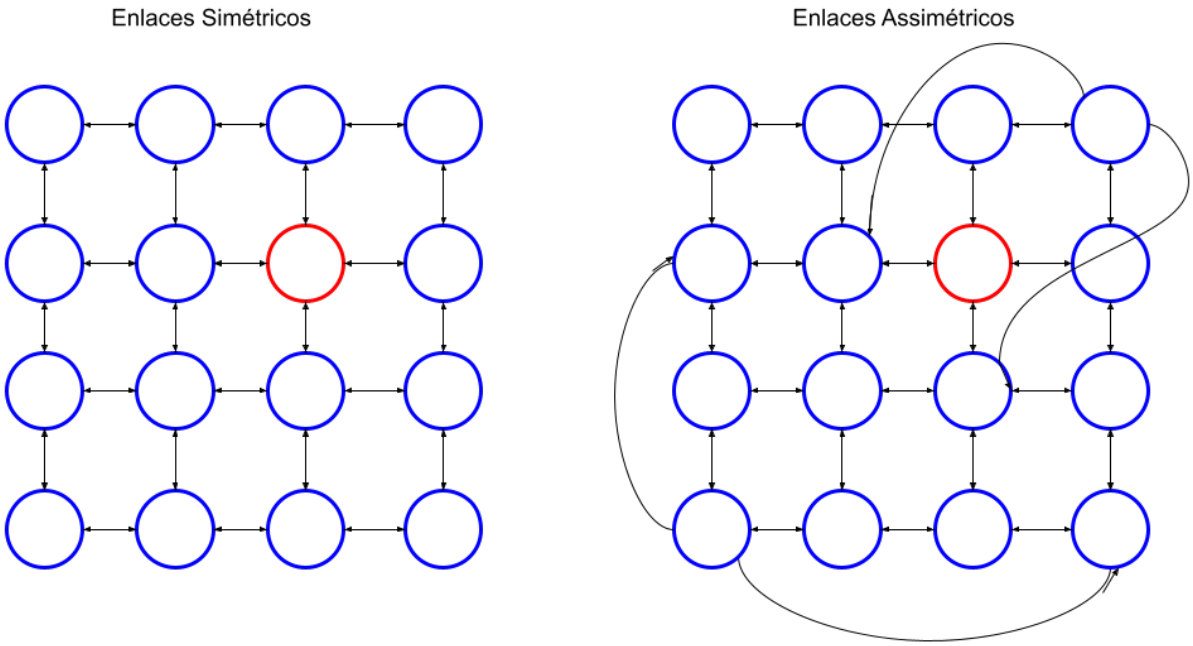

Figura 3: Enlaces simétricos / assimétricos

pouco planejados sem um padrão pré definido.

Portanto, em redes com enlaces assimétricos parâmetros como a relação de sinal-ruído (*signal to noise ratio*-SNR), indicação de qualidade do enlace (*link quality indication* - LQI), e taxa de entrega de pacote (*packet delivery ratio*-SDR) são, em geral, muito afetados. Além disso, o controlador devem ajutar as trocas de mensagens entre o eles e os nós da rede, para se compensar as diferenças de capacidade de transmissão de cada nó da rede e serem capazes de se comunicar de forma adequada.

2.5 Tipos de ataques e métodos de detecção

Assim como nas redes tradicionais, as redes definidas por software possuem diversas vulnerabilidades relacionadas com a segurança da rede, contudo com a proposta da separação do plano de dados e a centralização do plano de controle, novas formas de ataque devem ser exploradas e buscar novas formas de identificar tais ataques.

Na literatura [3], já é possível encontrar algumas das principais formas de ataques

de negação de serviço (buracos negros) e ataques de alteração de roteamento (buraco de minhoca) existentes, tanto no plano de controle quanto no plano de dados, e que são críticas em redes com recursos limitados.

Neste contexto, a utilização de tecnologias de identificação de ataques na SDN torna-se de extrema importância, podendo ser separadas em dois principais quesitos: a complexidade e a escalabilidade. As propostas de identificação de alto desempenho são em geral centralizadas e apresentam incompatibilidades com as limitações encontradas nas redes de sensores, o que afeta a escalabilidade da rede. Em contrapartida, as propostas híbridas em geral reduzem o tráfego de pacotes e os gargalos da proposta centralizada, contudo sua eficiência de identificação de ataques é afetada. Grande parte das vulnerabilidades existentes em um RSSF são baseadas no fato da comunicação ser sem fio e dos nós de sensores ficarem em locais sem segurança física ou monitoramento da rede. Portanto, os ataques em RSSF são divididos, basicamente, em dois tipos: ataques na camada física e ataques na camada de rede [3].

Os ataques na camada física incluem ataques de interferência do sinal de comunicação transmitido, esse tipo de ataque pode ocorrer quando um nó malicioso gera sinais aleatórios para impedir a comunicação entre nós do RSSF. Outra possibilidade de ataque na camada física seria danificar um nó sensor fisicamente, interrompendo a comunicação do nó na RSSF, ou danificar e substituir um nó por um outro malicioso.

Já os ataques na camada de rede estão associados ao roteamento de dados. Neste contexto as formas mais comuns de ataques estão associadas a alterar, repetir ou falsificar pacotes de controle de forma a criar *loops*, desvios (buracos de minhoca) ou negação de serviço (buracos negros). Nos ataques do tipo buracos negros um nó malicioso modifica a rota de vários pacotes da rede para passar por ele e serem descartados ou modificados. Em ataques do tipo *loop* um nó malicioso altera as rotas dos pacotes de modo a direcionar desvios ou *loops* para nós que possuem pouca energia (bateria) de forma a provocar atrasos e perdas de pacotes. Já no caso de buracos de minhocas, dois nós maliciosos são implementado na RSSF com frequências de rádio diferentes de forma a criar um túneis entre si, dessa forma os pacotes são enviados de um nó malicioso para o outro fazendo com que nós em diferentes partições acreditem serem vizinhos, o que causa problemas de convergência no roteamento da rede [3].

Por este motivo, diversas formas de detecção de ataques foram criadas, como maneira de encontrar e detectar ataques do tipo negação de serviços, vírus e worms em uma RSSF. Atualmente, para realizar essa detecção existem basicamente três tipos principais

de técnicas de detecção: as baseadas em assinatura, as baseadas em anomalia e as baseadas em especificação [4].

As baseadas em assinatura é muito eficiente em detectar ataques conhecidos, porém tem uma eficiência baixa contra ataques novos, uma vez que essa forma de detecção requer informações detalhadas sobre o comportamento do ataque.

Já as baseadas em anomalia é muito eficiente contra novos ataques, uma vez que não depende de parâmetros pré definidos. O método monitora, constantemente, o sistema e compara seu comportamento em relação a métricas, como consumo de energia ou número de pacotes de controle e nós vizinhos, com o comportamento esperado, e sempre que uma diferença significativa for detectada um alerta é acionado.

Por fim, as baseadas em especificação método realiza uma junção entre o método de baseadas em assinatura e baseadas em anomalia, uma vez que compara o comportamento da rede a partir de uma tabela pré definida, o que busca diminuir o casos de falso positivos que existem no caso de usar apenas baseadas em anomalia, porém, em contrapartida diminui a maleabilidade da detecção dos ataques.

3 ESPECIFICAÇÃO

Os ataques explorados baseiam-se em verificar o comportamento de um sistema de RSSF/IoT em SDN com enlaces assimétricos, quando incluído nós maliciosos com frequência de rádio de maior alcance, o que permite a comunicação deste nó com nós antes inalcançáveis. Para isso o trabalho se baseia-se na hipótese da não utilização da verificação de integridade e autenticidade na camada de dados da rede SDN.

3.1 Análise das vulnerabilidades em SDNs

Os ataques direcionados às redes SDN que foram explorados baseiam-se no fato dos dispositivos desta rede não serem capazes de realizar decisões sobre o encaminhamento de pacotes, dessa forma, sempre que um novo dispositivo não possuir regras sobre o encaminhamento dos pacotes novas regras de roteamento serão solicitadas ao controlador.

A partir disto diversos tipos de ataques podem ser explorados, por exemplo, um dispositivo maligno pode inundar o controlador da rede com solicitação de novas regras para o encaminhamento de pacotes causando uma sobrecarga no plano de controle e eventualmente interrompendo a comunicação SDN. Em redes de sensores sem fio esse ataque seria crítico uma vez que esse ataque pode acabar com a energia dos dispositivos de rede e causar sua desconexão. Os atacantes podem também inundar os dispositivos vizinhos com pacotes sem regras de encaminhamento definidos, e neste caso quem inunda a rede com solicitações de regras de encaminhamento são nós benignos. Neste caso também cada pacote com encaminhamento desconhecido significa uma nova regra o que satura as tabelas de roteamento depois de algumas solicitaçõe, o que diminui o taxa de entrega uma vez que regras que deveriam ser válidas não vão mais ser acrescentadas.

Os atacantes podem também se aproveitar dos pacotes que são utilizados na rede para o descobrimento da topologia da rede modificando sua informação e desinformando o controlador, por exemplo, manipulando os endereços de nós ou valores de métricas de roteamento. Isso é possível devido a falta de criptografia em redes de sensores sem fio

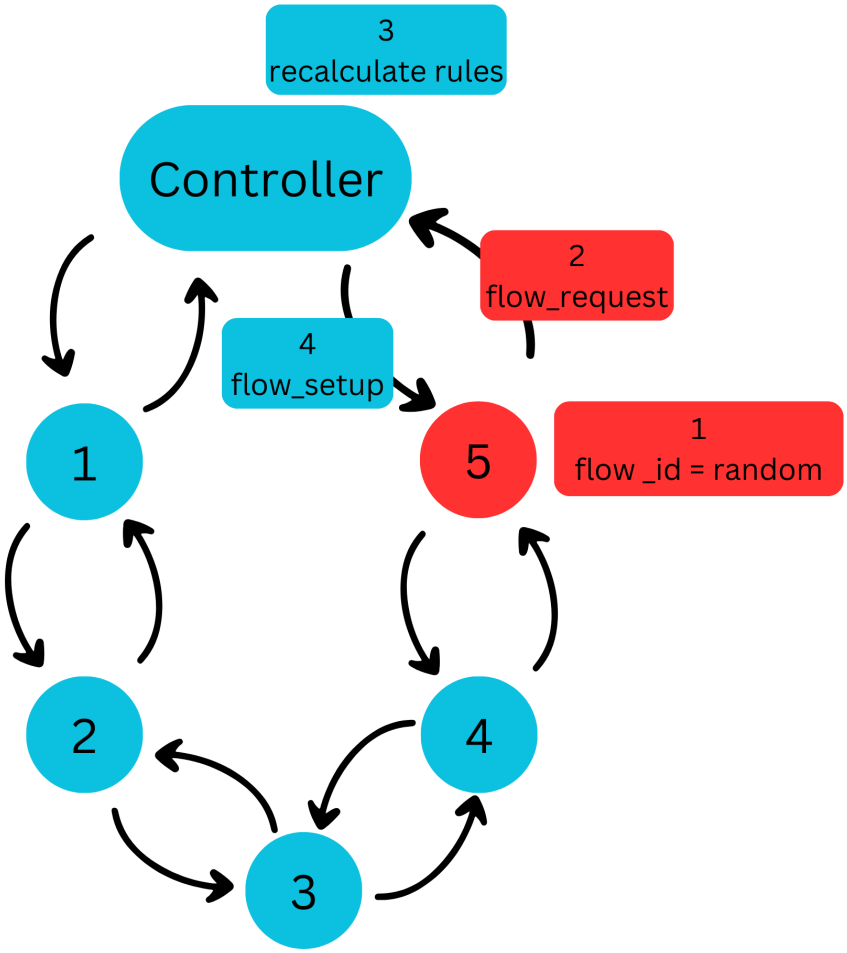

Figura 4: Diagrama de ataque do tipo FFR em enlaces simétricos

que são limitadas pela complexidade da rede, criptografia resulta em grande perdas de eficiência da rede.

Dado essas possibilidades, três ataque de negação de serviços em RSSF com SDN em enlaces simétricos serão explorado: *false flow request (FFR)*, *false data flow forwarding (FDFF)* e *false neighbor information (FNI)* [4]. O ataque FFR [Figura 4] tem o objetivo de atingir o controlador por meio da solicitação de múltiplos *flow rule request* ao controlador usando diferentes *flow IDs*, o controlador por sua vez processa os pacotes, calcula as novas regras e devolve um novo *flow setup* para o atacante. O objetivo principal do atacante, neste caso, é causar um overhead de processamento no controlador e aumentar o tráfego de pacotes para aumentar suas colisões e congestionamento na rede.

Já o ataques de FDFF [Figura 5] foca no ataque do controlador por meio de outros dispositivos da rede, para isso o atacante envia para os vizinhos pacotes de dados com *flow IDs* desconhecidos. Com isso, os vizinhos, ao checarem a tabela de roteamento e não encontrarem uma ação para o pacote recebido, pedem novas regras para o controlador, por meio de pacotes de *flow request*. O controlador, por sua vez, recalcula as regras e

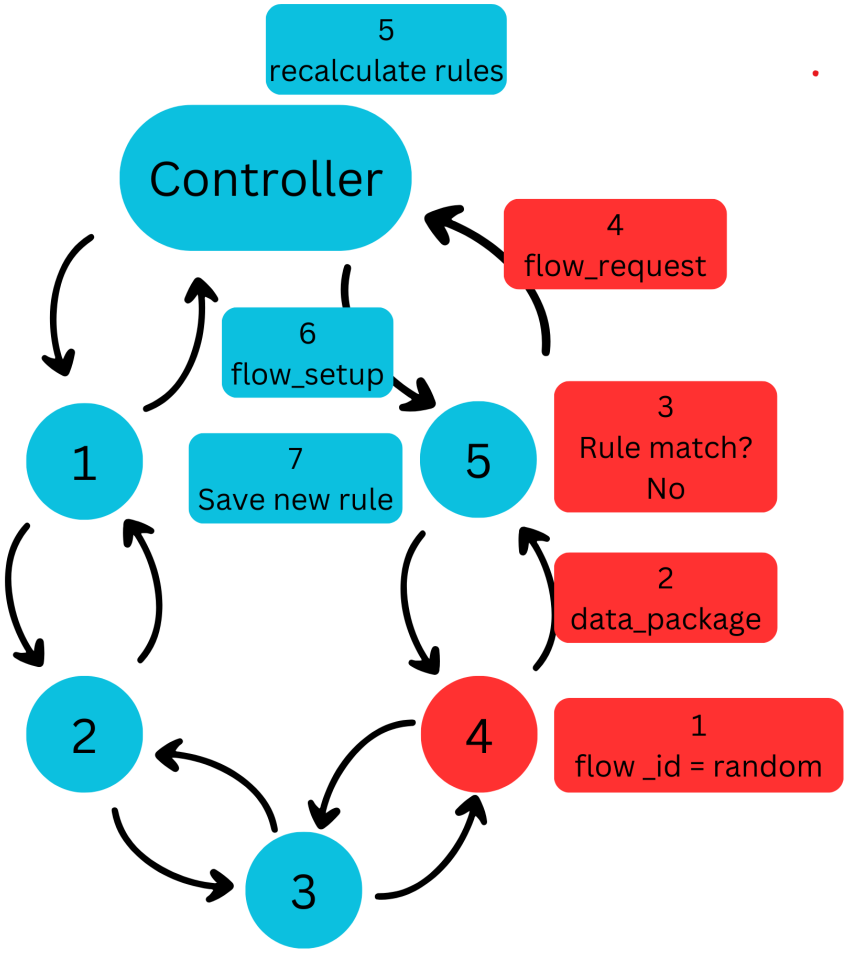

Figura 5: Diagrama de ataque do tipo FDFF em enlaces simétricos

envia aos vizinhos novos pacotes de *flow setup*. Assim como o ataque anterior, o objetivo principal do atacante é causar um overhead de processamento do controlador e aumentar o tráfego de pacotes para aumentar as colisões, porém neste ataque o nó malicioso faz isso por meio do ataque aos nós vizinhos.

Por fim, temos o ataque FNI [Figura 6] , que modifica os pacotes que contém informações dos vizinhos. O foco deste ataque é modificar ou as métricas de roteamento ou o número de identificação dos pacotes dos nós vizinhos, antes deste chegarem ao controlador. Dessa forma, o ataque leva o controlador a tratar informações falsas como verdadeiras e enviar novas regras de roteamento equivocadas para os nós.

3.2 Especificação do Ataque

Dado a análise destas possíveis vulnerabilidades em RSSF com SDN as propostas de ataques que foram definidas neste trabalho baseiam-se em avaliar as possibilidade de variações de ataque que podem ser implementados em redes SDN com enlaces assimétricos,

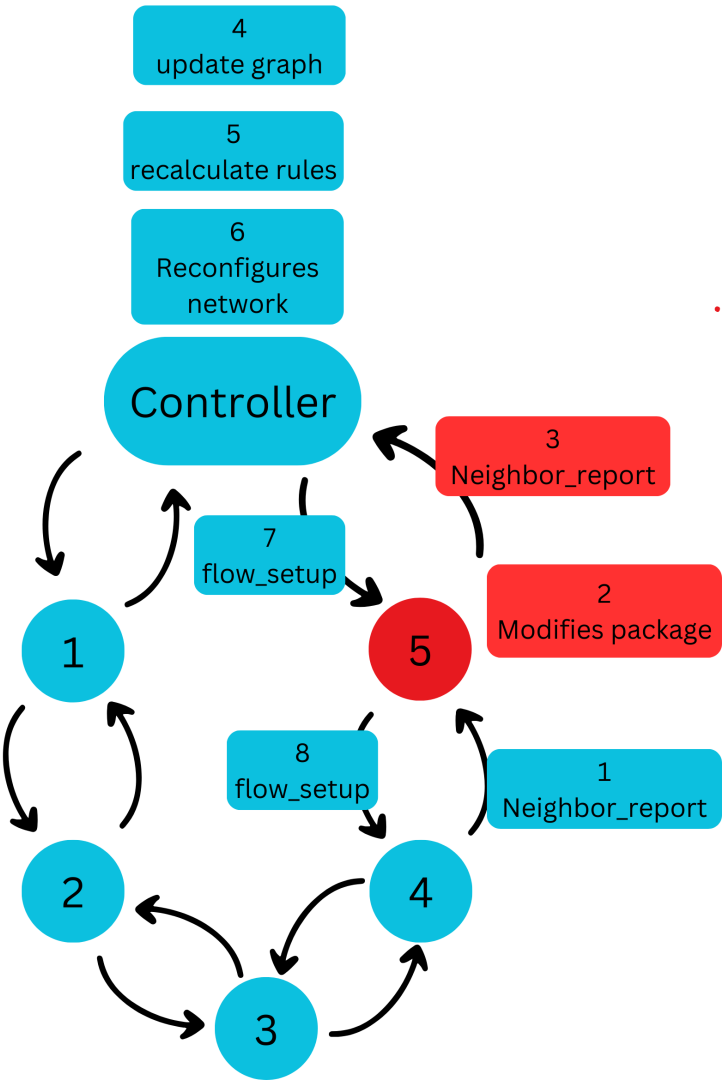

Figura 6: Diagrama de ataque do tipo FNI em enlaces simétricos

baseado-se para isso nos ataques de FFR, FDFF e FNI que foram propostos para enlaces simétricos definidos acima [4].

Portanto, os novos ataques visam, a partir da adição de um nó malicioso com potência de rádio de maior alcance, permitir a comunicação deste nó com nós antes inalcançáveis em redes simétricas. Dessa forma, verifica-se a possibilidade deste nó ser capaz de alterar uma ou mais rotas da rede gerando ataques do tipo buracos negros (negação de serviços) e buracos de minhoca.

Quando comparado a adição de um nó malicioso em enlaces assimétricos com os enlaces simétricos, esperasse que seja possível realizar as seguintes alterações nos ataque de FFR, FDFF e FNI.

Primeiramente, no caso do FFR [Figura 7] utilizando atacantes com potência de rádio maior, esperasse ser possível realizar *flow requests* do nó malicioso mais distante ao controlador diretamente, sem ser preciso, para isso, passar o *flow request* por outros nós vizinhos antes de chegar no controlador. Dessa forma, possivelmente o ataque será capaz de enviar mais rapidamente os "flow request" para o controlador e possivelmente inundar a rede de forma mais rápida.

Já no caso do FDFF [Figura 8], primeiramente será necessário validar se na implementação da rede SDN com enlaces assimétricos o atacante com potência de rádio maior terá acesso a tabela de vizinhos dos outros nós da rede. Partindo desta possibilidade, o novo ataque poderá permitir com que nós maliciosos enviem pacotes de dados errados para mais vizinhos e para vizinhos mais distantes, o que poderá causar uma inundação mais rápida da rede e um overhead de processamento mais rápido.

E, por fim, no caso do FNI [Figura 9] em enlaces assimétricos, será explorada a possibilidade de ataques do tipo buraco de minhoca. Onde o nó malicioso, ao alterar o "neighbor report" de um nós mais distantes, terá a possibilidade de alterar, não apenas os vizinhos diretos, como também poderá ser capaz de bagunçar a tabela de vizinhos mais distantes e, consequentemente, a tabela de roteamento de diversos nós da rede. Sendo assim capaz de mudar o roteamento dos nós para, por exemplo, sempre passarem pelo nó malicioso, ou fazer com que os pacotes sejam enviados para nós vizinhos equivocados.

3.3 Especificação da detecção do ataque

A implementação de algoritmos de autenticidade e integridade em sistemas de Redes de Sensores Sem Fio (RSSF), nos quais os recursos dos nós são predominantemente

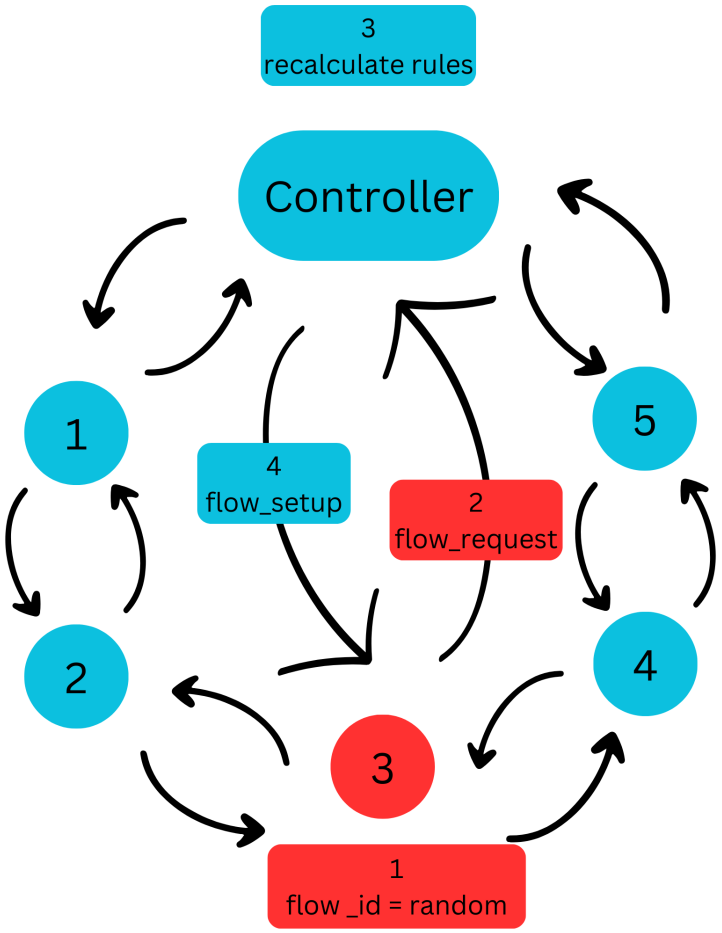

Figura 7: Diagrama de ataque do tipo FFR em enlaces assimétricos

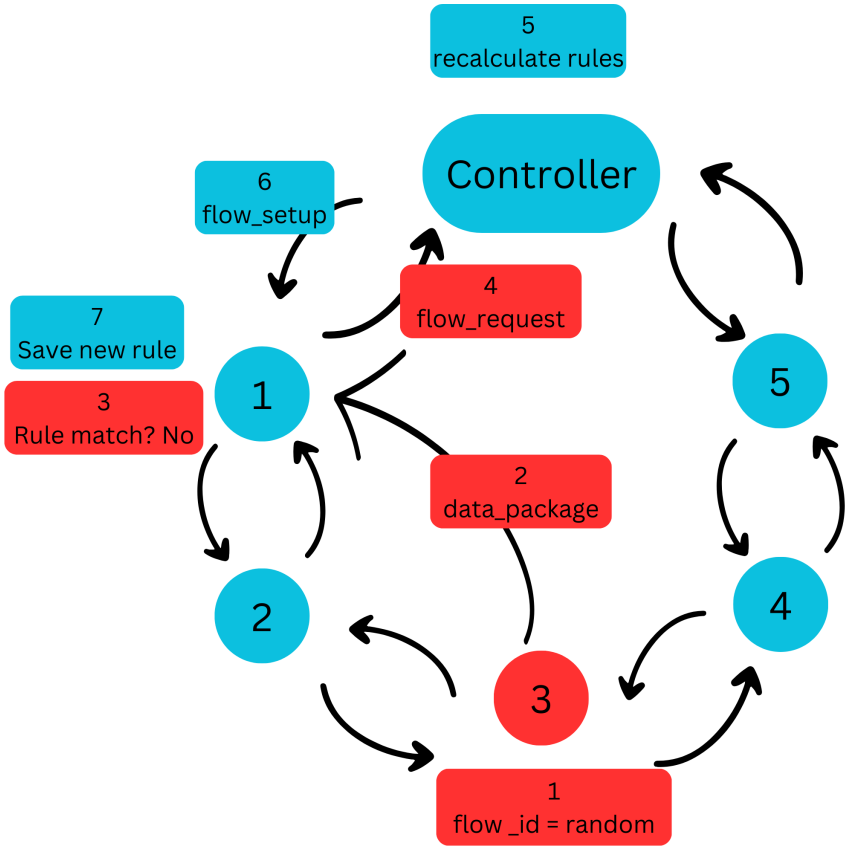

Figura 8: Diagrama de ataque do tipo FDFF em enlaces assimétricos

limitados, pode resultar em uma perda de desempenho significativa. Nesse contexto, a aplicação de novos algoritmos de detecção de ataques emerge como a opção ideal para preservar a eficiência da rede.

Portanto, este projeto utiliza como estratégia a implementação de verificações no plano de dados de maneira a detectar anomalias no roteamento de pacotes na rede. Para isso, o trabalho baseia-se na proposta de cooperação de todos os elementos da rede, inspirado no paradigma de multi-agentes (WOOLDRIDGE, 2009)[5]. Primeiro foram definidos os tipos de agentes existentes na rede SDN e como eles interagem entre si. Em seguida foram definidos o que são cosiderados anomalias na rede e como detecta-las, e por fim foram definidos os critérios de classificação destas anomalias.

3.3.1 Arquitetura de multi-agentes [5]

Na definição da arquitetura de multi-agentes (WOOLDRIDGE, 2009)[5], são utilizados todos os elementos da rede SDN em cooperação para determinar se a rede está em ataque de negação de serviço, determinar o tipo de ataque e determinar qual o nó responsável pelos ataques, sendo os elementos da rede definidos por: Security Manager,

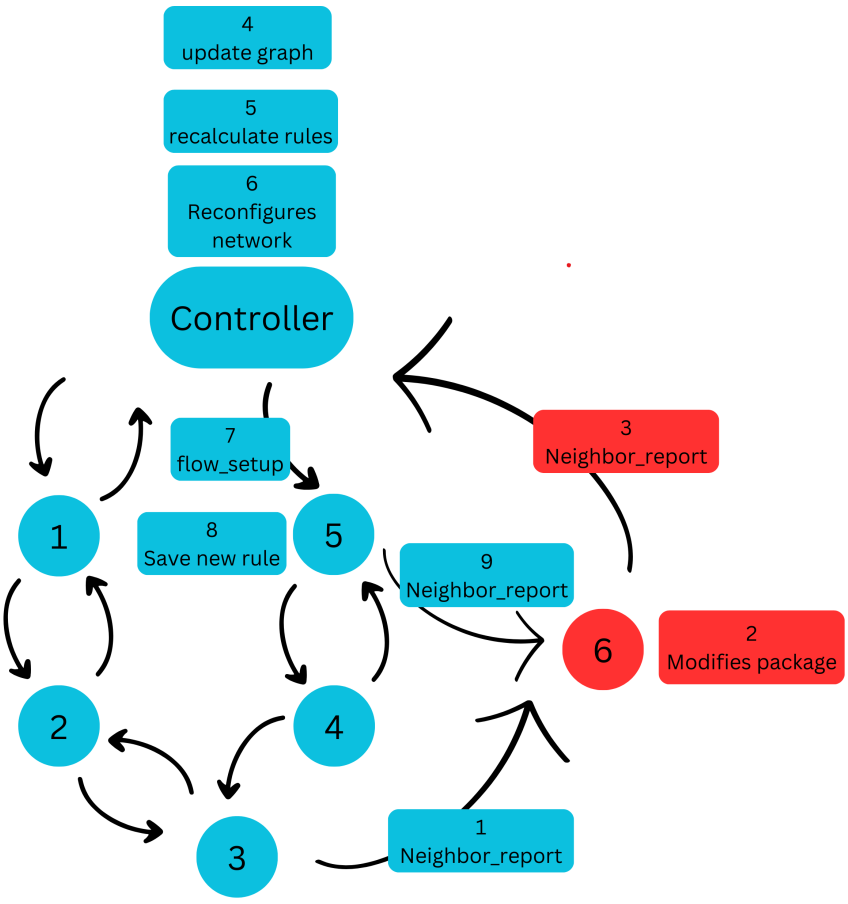

Figura 9: Diagrama de ataque do tipo FNI em enlaces assimétricos

dispositivos de sensores, gerente de desempenho e o controlador da SDN.

O gerente de segurança é responsável pelas decisões relacionadas a segurança da rede, este elemento determina quando e quais anomalias são causadas por ataques de negação de serviço, determina o tipo de ataque e identifica o nó malicioso. Para isso eles usam as informações provenientes dos outros elementos da rede.

Já os dispositivos de sensores monitoram, constantemente, as suas métricas individuais, como: a utilização de módulo de rádio, uso de processamento e transmissão e recebimento de pacotes. Dessa forma, quando um sensor detectar alguma anomalia em um ou mais métricas ela levanta um alarme para o Security Manager.

Por outro lado, o Controlador SDN é responsável por fornecer informações de gráficos da rede para o Security Manager e reconfigura a rede de acordo com as instruções da Security Manager.

Por fim, o Performance Manager se responsabiliza por coletar todos os dados dos sensores da rede e do Controlador da SDN e calcular métricas de performance da rede, em seguida ele é responsável por fornecer para o Security Manager quando necessárias. Além disso, este elemento da rede ajuda o Security Manager a detectar anomalias por meio das métricas coletadas.

Uma vez definidos os agentes responsáveis pela detecção de ataques na rede é preciso verificar como esses a gente interage entre si para a detecção de DoS ataques. Nesse tipo de configuração do dispositivo de sensores se comunicam diretamente com o Security manager indicando se algum sensor possui métricas alteradas ou não, se o Security manager determinar que era um falso alarme informa ao sensor para continuar sua atuação normalmente. Já a interação do Security manager com a rede se baseia receber informações do Performance Manager ou dos dispositivos sensores e caso tenha uma detecção de ataque pede informações para o SDN Controller e Performance manager sobre configurações executadas recentemente nos nós ou seus vizinho ou configurações recentes na rede e decide a partir destes dados se a anomalia observada deve ser considerada um ataque ou não.

3.3.2 Change point (CP)

Para buscar detectar os ataques propostos, inicialmente, a técnica que será utilizada juntamente com a utilização dos elementos de redes definidas acima, será a detecção de anomalias baseadas em análise de *Change Point* (CP) [4], que procura verificar comportamentos anômalos na rede e a partir da sua análise detectar possíveis ameaças.

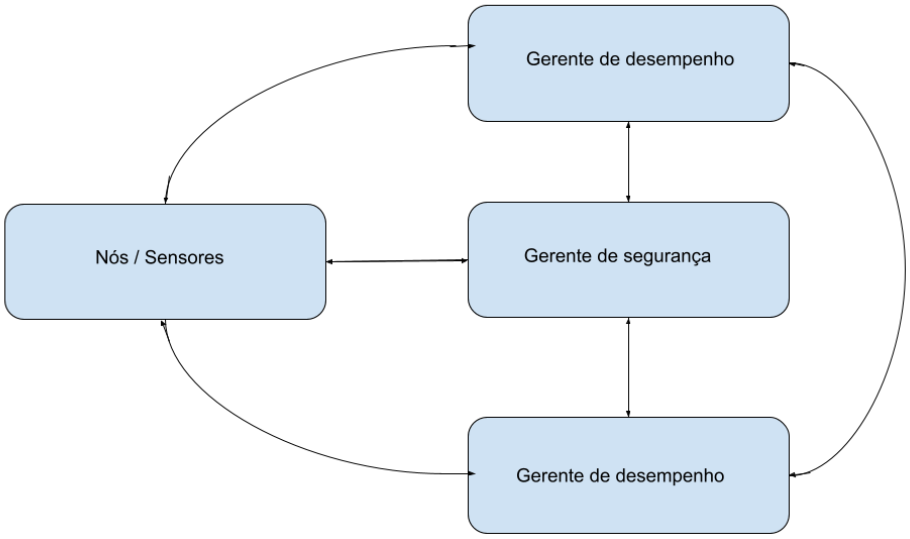

Figura 10: Elementos de detecção em uma rede SDN com arquitetura de multi-agentes

Essa proposta se baseia no fato dos sensores e Security manager serem responsáveis por detectar anomalias, dessa forma eles executam análises de algoritmo baseado em Change Point que utilizam métricas de taxa de entrega e controle de overhead de pacotes que, geralmente, são impactadas em ataques de DoS.

Essa técnica propõe a utilização de duas fases, a fase off-line e a fase on-line. A fase off-line é o período de treino do algoritmo e a fase on-line utilização deste algoritmo treinado para a detecção de anomalias. Contudo, como em RSSF os recursos são limitados será utilizado apenas a fase on-line que se mostrou eficiente para as características da nossa rede.

A escolha de, utilizar a técnica de Change Point detection, se deve a alguns fatores, entre eles a ideia de se utilizar um algoritmo de baixa complexidade, alta taxa de sucesso e de possibilidade de encaixar este algoritmo em RSSF com recursos limitados, além de ter sido a proposta de detecção utilizada para a verificação deste ataques em redes de enlace simétricos [4].

3.3.3 Classificação simples de anomalias

Para a classificação das anomalias o trabalho vai se basear na hipótese de uma rede regime, sem muitas modificações de controle e reconfiguração de rede após a sua imple-

mentação inicial, supondo ainda um número fixo de nós durante toda sua operação. Considerando essa hipóteses a RSSF a serem simuladas deve permanecer estável e o Security manager declara a rede sobre ataque quando uma anomalia em um metrica centralizada é detectada ou quando um atacante é identificado.

4 DESENVOLVIMENTO DO TRABALHO

4.1 Tecnologias Utilizada

Como base para o desenvolvimento deste trabalho foi utilizado a tecnologias IDIT-SDN (Intrusion Detection Framework for software-defined Wireless Sensor Networks) [6]. Este código aberto utiliza-se do IT-SDN e do Contiki-OS para simular uma RSSF definida por software e detecta, utilizando-se da técnica de *on-line Change Point*, possíveis ataques na rede. Além disso, este código gera relatórios de detecção de ataques, tanto no controlador, quanto nos nós da rede.

Este código utiliza-se da programação em C para descrever uma RSSF no Contiki-OS, dessa forma é possível modificar e adicionar comportamentos ao código com características específicas para a implementação de diferentes projetos.

4.1.1 Especificação da tecnologia utilizada

A tecnologia IDIT-SDN (Intrusion Detection Framework for Software-Defined Wireless Sensor Networks) [6] baseia-se na detecção de ataques em redes SDN utilizando-se de dois detectores de *Change Point*. Estes detectores funcionam em paralelo com o objetivo de monitorar, em uma amostragem de tempo predefinida, a sobrecarga de pacotes de controle de pacotes e a taxa de entrega de pacotes de dados.

Se o detector responsável pelo monitoramento da sobrecarga de pacotes de controle for acionado, o ataque será classificado como do tipo FDFF. Contudo, se o detector que monitora a taxa de entrega de pacotes de dados for acionado, o ataque será categorizado como do tipo FNI.

As detecções de ataques via *Change Point* são aplicadas tanto na camada de controle (Csec) quanto na camada de nós (Nsec). Dessa forma, utiliza-se da técnica de segurança de arquitetura de multi agentes.

4.2 Projeto e Implementação

Para a implementação deste projeto, foram realizadas modificações no código aberto IDIT-SDN [6] com o objetivo de realizar ataques do tipo FDFF, no qual nós maliciosos são capaz de enviar "False Data Flow"para seus vizinhos próximos e/ou para nós mais distantes. Uma vez implementadas as modificações no código, foram propostos e simulados 4 cenários de ataques para validação e comparação do impacto na segurança da rede.

4.2.1 Parâmetros de rede, segurança e simulação

Para efeitos de comparação, foram conduzidos 4 cenários de simulação, nos quais foram utilizados os parâmetros de segurança e de rede preestabelecidos pelo código do IDIT-SDN [6], conforme ilustrado nas tabelas 1 e 2. Tais parâmetros foram desenvolvidos e são considerados otimizados para a detecção de CP, de ataques do tipo FDFF e FNI em enlaces simétricos, e desejamos comparar e validar esse simulador para enlaces assimétricos

Quanto à configuração inicial da rede, esta segue a topologia apresentada na Figura 11. Essa configuração consiste em uma Rede de Sensores Sem Fio (RSSF) que inclui nós sorvedouros (representados em amarelo), um controlador(representado em verde) e nós maliciosos (representados em azul). Para todas as simulações, essa topologia será mantida, contudo será modificados o tamanho da rede, o número de nós maliciosos e o número de nós que sofrem os ataques.

Em relação aos parâmetros de simulação, serão mantidos: o tempo de simulação de 5 horas, a taxa de tráfego de dados, o tempo de início do ataque, o tempo de amostragem para deteção de CP nos nós e a janela de amostragens utilizada para detecção de CP no controlador. Conforme as tabelas 1, 2 e 3.

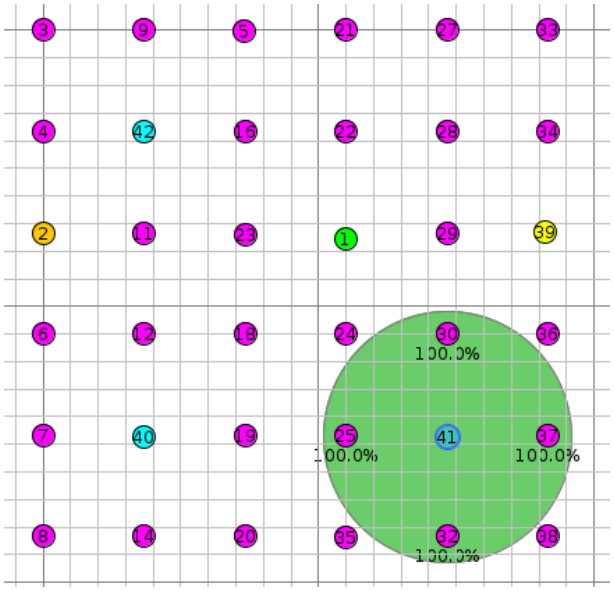

Figura 11: Exemplo de topologia de RSSF com 36 nós

Tabela 1: Parâmetros do Nsec

NSec parâmeters	**Value**
Janela de monitoramento (m win)	200
Janela de detecção (d win)	50
Período de amostragem	60s
Valor crítico (ca)	2.82
Sensibilidade (g)	0

Tabela 2: Parametros do Csec

Parameter	**Value**
Período de monitoramento	60s
S SKIP	10 amostras
T_WIN	210 amostras
GAMMA	0.45
S_val	0.95

Tabela 3: Parâmetros de Simulação

Parâmetro	**Valor**
Tempo de simulação	18000s
taxa de tráfego de dados	1 packet/min [”payload”: 10 bytes]
Início do ataques	14000s

4.3 Testes e Avaliação

Uma vez modificado o código [7], para o ataque de FDFF descrito, e validado seu funcionamento, foram realizadas diversas variações da simulação para verificar o impacto de nós com frequência de rádio maior sobre a segurança da rede IDIT-SDN desenvolvida.

Com este propósito, foi discutido e desenvolvido um planejamento de 4 cenários de simulações como o objetivo de se ter um panorama geral do impacto da adição destes ataques na rede. Para cada cenário proposto foram realizadas 5 simulações por item de cenário, e cada simulação foi validadas de acordo com métricas pré estabelecidas. Uma vez avaliada cada simulação foram ralizadas as médias simples das 5 simualçoes.

4.3.1 Métricas de avaliação

As métricas que foram utilizadas para a validação e comparação das simulações, foram baseadas nos relatórios gerados pelas simulações do IDIT-SDN [6]. Tais relatórios, avaliam tanto à segurança na camada do Controlador(Csec) e quanto a segurança na camada dos nós (Nsec).

4.3.1.1 Tabela de métricas do controlador(Csec)

Para o controlador, foram avaliadas as seguinte métrica: a taxa de detecção de ataques do tipo FDFF, a taxa de detecção de ataques do tipo FNI, a taxa de detecção de *change point* e a taxa de detecção de falsos negativos [tabela 4]

A taxa de detecção de ataques, tanto do tipo FNI quanto FDFF, são calculadas pelo código durante a simulação, por meio das seguintes comparações. Se houver uma sobrecarga de pacotes de controle superior a 100 pacotes, o ataque será classificado como FDFF. Da mesma forma, se for observada uma taxa de entrega de pacotes superior a 200 pacotes, o ataque será classificado como FNI. Essas métricas são derivadas de uma janela de amostragem predefinida, composta por 210 amostragens temporais. Cada amostragem representa um perido de amostragem de 60 segundos dos nós do controlador.

Já a taxa de detecção de *change point* (CP), é calculada pelo código durante a simulação por meio da comparação do valor do fator de detecção (DT) e em relação ao valor crítico (ca). O DT é calculado usando o método de soma cumulativa de janela de amostragem predefinida, composta por 210 amostragens temporais. Visando identificar mudanças significativas no sistema monitorado. Se o DT ultrapassar um determinado

limiar (ca, valor crítico), isso indica um possível ponto de mudança e um alarme de CP é acionado.

Por último, será verificada a taxa de detecção de falsos negativos, que será calculada subtraindo o número total de ataques realizados(Nt) do número total de ataques detectados(Nd) e dividindo essa subtração pelo número total de ataques realizados(Nt). Para essa análise foi utilizado a valor em porcentagem, portanto o valor obtido foi multiplicado por 100. Além disso, foi considerado 1 ataque no controlador como sendo o ato de um nó malicioso enviar fluxo de dados falso para os seus 4 ou mais vizinhos correspondentes.

Tabela 4: Métricas do controlador(Csec)

Métricas do controlador(Csec)	**Descrição**
Taxa de ataques de FDFF detectados	Verifica a sobrecarga de pacotes de controle
Taxa de ataques de FNI detectados	Verifica a taxa de entrega de pacotes
Taxa de ataques de CP detectados	Compara o o fator de deteção com um valor críticos
Taxa de detecção de falso negativo	$((Nt$ - $Nd)$ / Nt*100

4.3.1.2 Tabela de métricas dos nós(Nsec)

Para a camada dos nós, foi validada a taxa de detecção de *change point*, a taxa de detecção inicial média e a taxa de detecção de falsos negativos [tabela 5].

A taxa de detecção de CP, assim como no controlador, é calculada pelo código durante a simulação por meio da comparação do valor do fator de detecção (DT) e em relação ao valor crítico (ca). O DT é calculado usando o método de soma cumulativa de uma amostragem de tempo de 60 segundos, visando identificar mudanças significativas no sistema monitorado. Se o DT ultrapassar um determinado limiar (ca, valor crítico), isso indica um possível ponto de mudança e um alarme de CP é acionado.

Já a taxa de detecção inicial média, é calculada pela diferença entre o tempo da primeira detecção de CP(Td) e o tempo do início do ataque(Ti).

E por último, a taxa de detecção de falsos negativos, que será calculada subtraindo o número total de ataques realizados(Nt) do número de ataques detectados(Nd) e dividindo essa subtração pelo número total de ataques realizados(Nt). Para essa análise foi utilizado a valor em porcentagem, portanto o valor obtido foi multiplicado por 100. Além disso, 1 ataque no nó é considerado quando um nó recbe um fluxo de dados falso de um vizinho, portanto cada "false flow"que for enviado pelo nó malicioso é considerado 1 ataque no nó.

Tabela 5: Métricas dos Nós(Nsec)

Métricas dos nós(Nsec)	**Descrição**
Taxa de ataques de CP detectados	Compara o o fator de deteção com um valor críticos
Taxa de detecção inicial média	Td - Ti
Taxa de detecção de falso negativo	((Nt - Nd) / Nt))*100

4.3.2 Cenários de Avaliação

Uma vez estabelecidas as métricas de avaliação, foram desenvolvidos os seguintes cenários de simulação. Os quatro cenários propostos são: A variação da proporção dos nós vizinhos atacados e nós não vizinhos, a variação do tamanho da rede, a variação do número de nós atacados por atacantes e a variação do número de atacantes.

4.3.2.1 Primeiro cenário, variação da proporção dos nós vizinhos atacado e nós não vizinhos

Neste primeiro cenário, foi avaliado o impacto de enlaces assimétricos em uma rede com 36 nós fixos e com 3 nós maliciosos fixos, mas variando os nós a serem atacados. Na primeira simulação, os enlaces são simétricos, e os nós maliciosos atacam, apenas, os nós vizinhos. Em seguida, foi alterada a proporção de nós vizinhos e nós não vizinhos atacados, onde 3 nós vizinhos foram atacados e um nó mais distante foi atacado. Posteriormente, foram atacados 2 nós vizinhos e 2 nós não vizinhos, e assim por diante, conforme estabelecido pela tabela 6.

Tabela 6: Variação da proporção dos nós vizinhos atacado e nós não vizinhos

Tamanho da rede	**Número de atacantes**	**Número de atacados por atacantes**	**Nós vizinhos**	**Nós não vizinhos**	**Simulação**
36	3	4	4	0	1
36	3	4	3	1	2
36	3	4	2	2	3
36	3	4	1	3	4
36	3	4	0	4	5

4.3.2.2 Segundo cenário, variando tamanho da rede

Neste segundo cenário, foi avaliado o impacto da simulação de ataques assimétricos em redes de tamanhos variados. Para isso, a simulação foi realizada com 3 atacantes fixos

em redes de 100 nós e 225 nós, comparando o impacto da simulação em enlaces simétricos e enlaces assimétricos, conforme estabelecido pela tabela 7.

Tabela 7: Variando tamanho da rede

Tamanho da rede	**Número de atacantes**	**Número de atacados por atacantes**	**Nós vizinhos**	**Nós não vizinhos**	**Simulação**
100	3	4	4	0	1
100	3	4	0	4	2
225	3	4	4	0	3
225	3	4	0	4	4

4.3.2.3 Terceiro cenário, variando número de atacados por atacantes

Neste cenário, foi avaliado o impacto do aumento do número de nós não vizinhos que estavam sendo atacados. Portanto, em uma rede de 36 nós fixos, foram realizadas simulações com enlaces assimétricos onde 5 nós não vizinhos serão atacados, e em seguida 6, 7 e 8 nós não vizinhos foram atacados, respectivamente. Conforme estabelecido pela tabela 8.

Tabela 8: Variando número de atacados por atacantes

Tamanho da rede	**Número de atacantes**	**Número de atacados por atacantes**	**Nós vizinhos**	**Nós não vizinhos**	**Simulação**
36	3	5	0	5	1
36	3	6	0	6	2
36	3	7	0	7	3
36	3	8	0	8	4

4.3.2.4 Quarto cenário,Variando número de atacantes

Neste último cenário, foi avaliado o impacto do aumento do número de nós maliciosos em uma rede de 36 nós fixos. Neste caso, apenas nós não vizinhos serão atacados, e um número fixo de 4 nós por atacante foi atacado. Conforme estabelecido pela tabela 9.

Tabela 9: Variando número de atacantes

Tamanho da rede	**Número de atacantes**	**Número de atacados por atacantes**	**Nós vizinhos**	**Nós não vizinhos**	**Simulação**
36	4	4	0	4	1
36	5	4	0	4	2
36	6	4	0	4	3
36	7	4	0	4	4

5 RESULTADOS

Após a realização de todas as simulações para cada cenário proposto, foi possível entender melhor os impactos que a adição de ataques de tipo FDFF em enalces assimetricos podem causar em uma rede SDN com recursos limitados.

5.1 Resultados por cenário

Para cada cenário, foram realizadas as simulações correspondentes, com o objetivo de validar o impacto dos ataques num contexto geral. Foram realizadas 5 simulações para cada item da tabela e foram tiradas as medias simples das métricas para gerada as tabela de resultados. As tabelas foram dividas entre métricas de segurança nos controladores (Csec) e dos nós (Nsec).

5.1.1 Primeiro cenário, conclusões

Para o primeiro cenário (tabela 10), com relação ao impacto dos ataques na camada de controle (Csec), foi possível verificar que quanto mais nós não vizinhos foram atacados, menor foi a taxa de detecção de ataques do tipo FDFF. Contudo, quanto as demais métricas de análise, não foi possivel verificar uma relação direta quanto ao aumento de nós não vizinhos atacados e o impacto destes ataques na rede.

Tabela 10: Impacto nos controladores

Simulações	**FDFF**	**FNI**	**CP Csec**	**Falso Negativo (%)**
1	62,2	6,6	68,8	64,71794872
2	61,8	33,8	95,6	50,97435897
3	60,2	15,2	75,4	61,33333333
4	57,4	2	59,2	69,64102564
5	27,8	15,6	43,4	77,74358974

Já quanto as métricas de segurança nos nós da rede (Nsec) (tabela 11), foi possível

verificar uma relação direta entre o aumento do número de ataques em nós não vizinhos e a queda do número de CP detectados. Além disso, para o caso onde foram apenas atacados nós mais distantes, houve um aumento cosiderável no valor de taxa de detecção inicial média das simulações.

Tabela 11: Impacto nos nós

Simulações	**CP Nsec**	**Taxa de detecção inicial média (Segundos)**	**Taxa de detecção de falso negativo (%)**
1	20,8	240,6	97,33333333
2	19,6	235,6	97,48717949
3	20,4	278,4	97,38461538
4	14	257	98,20512821
5	9,6	443,8	98,76923077

Após a análise destes resultados foi possível concluir que, com o aumento dos ataques de FDFF em nós mais distantes o controlador da rede teve mais dificuldade em verificar a sobrecarga de pacotes no controlador da rede. Já os nós da rede, demoraram mais para perceberem uma variação do comportamento da rede e tiveram mais dificuladades para encontrarem CP na rede.

5.1.2 Segundo cenário, conclusões

Neste segundo cenário(tabela 12), foi avaliado o impacto dos ataques em enlaces assimétricos em redes com 100 e 225 nós. Com relação ao impacto dos ataques na camada de controle (Csec), foi possível notar que nos dois casos, onde a rede foi atacada por apenas enlaces assimétrios, a taxa de ataques do tipo FDFF detectados forma menor quando comparadas ao ataques em enlaces simétricos, assim como havia sido validado no primeiro cenário de simulações. Além disso, nos dois casos houve um aumento do número de ataques do tipo FNI detectados e de CP detectados.

Tabela 12: Impacto nos controladores

Simulações	**FDFF**	**FNI**	**CP Csec**	**Falso Negativo (%)**
1	61,8	8,2	70	64,1025641
2	58,4	49,8	108,2	44,51282051
3	62	27,2	89,2	54,25641026
4	56	51	107,6	44,82051282

Já quanto as métricas de segurança dos nós da rede (Nsec) (tabela 13), foi possível verificar que, nos casos de ataques em enlaces assimétricos, independente do tamanho da

rede, a taxa de detecção de CP foram menores e houve um pequeno aumento da taxa de detecção inicial média. Assim como havia sido validado no primeiro cenário de simulações.

Tabela 13: Impacto nos nós

Simulações	**CP Nsec**	**Taxa de detecção inicial média (Segundos)**	**Taxa de detecção de falso negativo (%)**
1	20,6	229,4	97,35897436
2	13,4	292,8	98,28205128
3	21,2	258,2	97,28205128
4	10,6	350	98,64102564

Desta forma, neste segundo cenário foi possivel validar que, independente do aumento do tamanho da rede, o controlador continuou tendo uma dificuldade maior de detectar a sobrecarga de pacotes de controle na rede. Por outro lado, o controlador foi capaz de identificar uma taxa maior de CP e considerou mais ataques como do tipo FNI, por receber que houve um aumento da taxa de entrega de pacotes na rede. Quanto aos nó da rede foi possível perceber que eles tiveram dificuldade de perceber anomalias na rede, e demorarem um tempo maior para perceberem os primeiros ataques na rede.

5.1.3 Terceiro cenário, conclusões

Neste terceiro cenário (tabela 14 e 15), foi avaliado o impacto do aumento do número de nós que sofrem o ataque do tipo FDFF. E, ao contrário do que era esperado, não foi possível notar uma diferença significa nas métricas analisadas pelo controlador e pelos nós com o aumento de nós não vizinhos que foram atacados.

Tabela 14: Impacto nos controladores

Simulações	**FDFF**	**FNI**	**CP Csec**	**Falso Negativo (%)**
1	57,8	49,2	107	45,12820513
2	57	44,2	101,2	48,1025641
3	58,8	16,4	75,2	61,43589744
4	55,8	67	122,8	37,02564103

Então podemos concluir, pelas tabelas, que idependente do aumento do número de nós não vizinhos sendo atacados não houve um aumento de detecção na taxa de ataques do tipo FNI, FDFF e de CP detectados.

Tabela 15: Impacto nos nós

Simulações	CP Nsec	Taxa de detecção inicial média (Segundos)	Taxa de detecção de falso negativo (%)
1	12	258,4	98,76923077
2	10,2	295,2	99,12820513
3	9,8	237	99,28205128
4	13,2	241	99,15384615

5.1.4 Quarto cenário, conclusões

Neste quarto cenário (tabela 16), onde foi avaliado o impacto do aumento de nós maliciosos na rede com enlaces assimétricos, foi possivel nota que. Com relação ao impacto dos ataques na camada de controle (Csec), com o aumento de nós malicioso a quantidade de taxa de detecção de CP detectados aumentou proporcionalmente, e conseguentemente a taxa de falsos negativos diminuiu.

Tabela 16: Impacto nos controladores

Simulações	FDFF	FNI	CP Csec	Falso Negativo (%)
1	59,6	49,8	109,4	57,76061776
2	60,6	61,8	122,4	52,74131274
3	60,4	64,8	125,2	51,66023166
4	61,4	65,2	126,6	51,11969112

Já quanto as métricas de segurança dos nós da rede (Nsec) (tabela 17), foi possível verificar que, nos casos de ataques em enlaces assimétricos, quanto mais nós maliciosos exitirem na rede maior é a quantidade de CP detectado por nó da rede. além disso foi possivel notar um aumento na taxa de detecção inicial média dos ataques.

Tabela 17: Impacto nos nós

Simulações	CP Nsec	Taxa de detecção inicial média (Segundos)	Taxa de detecção de falso negativo (%)
1	8,2	320,2	99,21
2	11	322,4	98,94
3	14,2	332	98,63
4	15,6	340	98,53

Portanto foi possível concluir que, neste cenário o aumento do numero de nós malisiosos não dificulta de forma consideravel a detecção da sobrecarga de pacotes de entregas no controlador nem a deteção do aumento de taxa de entrega de pacotes, contudo a rede

foi sim capaz de observar um aumento de detecção de anomalias tanto no controlador quanto nos nós da rede.

5.2 Conclusões

Após a análise das simulações dos quatro cenários propostos, foi possível verificar que o fator que causou um impacto mais significativo na rede foi a transição do ataques com enlaces simétricos para ataques com enlaces puramente assimétricos. Com está transição foi possível verificar que o controlador teve reconheceu mais ataques que causam a sobrecarga da entrega de pacotes na rede e ataques que aumentam a taxa de entrega dos pacotes. Consequentemente, a detecção de anomalias na rede pelo uso do CP aumentou e o aumento da taxa de detecção de entrega de pacotes foi notória.

Contudo, ao contrário do que era esperado, não foi possível verificar uma relação direta entre o aumento de nós não vizinhos que foram atacados e um impacto destes ataques na rede. O mesmo foi observada para o aumento da quantidade de nós maliciosos na rede, não houve um aumento consideravel de detecação de CP com o aumento de nós maliciosos na rede.

6 CONSIDERAÇÕES FINAIS

Com a realização deste projeto de conclusão de curso, foi possível compreender o funcionamento do novo paradigma de redes definidas por software (SDN) e os desafios de segurança que esta rede traz, por possuir um plano de dados separado do plano de controle.

Além disso, possibilitou compreender a importância da utilização destas redes SDN em aplicações com recursos limitados, e suas vantagens em redes que requerem uma maior flexibilidade e escalabilidade de recursos, como é o caso das RSSF para IoT.

Este projeto possibilitou, também, o entendimento sobre as tecnologias modernas que são utilizadas para a detecção de ataques em redes. Como por exemplo a utilização de multi-agentes e técnicas de detecção de anomalias em sistemas (change point) .

Por fim, por meio dos ataques desenvolvidos e simulações realizadas, foi possível compreender o impacto que ataques do tipo FDFF causam em enlaces assimétricos, tais como os fatores que tornam estes ataques mais ofensivos na rede.

6.1 Objetivos atingidos

O objetivo principal deste trabalho foi atingido, uma vez que foi possível analisar como enlaces assimétricos em RSSF podem viabilizar novos tipos de ataques em redes definidas por software.

Além disso, o objetivo de validar por meio de simulações os ataques do tipo FDFF em enlaces simétricos e assimétricos também foi atingido. Uma vez que, por meio dos 4 cenários propostos e das simulações realizadas foi possível validar e comparar que a adição de nós maliciosos em enlaces assimétricos causaram sim um impacto mais ofensivo na rede quando comparados com os mesmos ataques em enlaces simétricos.

6.2 Trabalhos futuros

Apesar de ter atingido o objetivo principal, este trabalho ainda oferece possibilidades de continuação. A implementação e simulação do ataque FDFF em enlaces assimétricos foram realizadas, comparando os resultados com o mesmo ataque em enlaces simétricos. No entanto, não foram implementados ataques do tipo FNI e FFR, abrindo espaço para o desenvolvimento de outros ataques em enlaces assimétricos.

Para uma validação mais abrangente dos ataques já implementados, novos cenários de simulação podem ser adicionados. Por exemplo, seria válido realizar simulações em que os nós maliciosos atacam diferentes nós não vizinhos a cada chamada do ataque FDFF. No trabalho atual, os mesmos nós não vizinhos são atacados a cada chamada do ataque.

Outra possibilidade seria a inclusão de novas métricas nas simulações. Essa adição pode proporcionar novos resultados nos cenários propostos e, consequentemente, gerar novas conclusões sobre os ataques realizados. Por exemplo, a introdução da métrica de taxa de detecção de falsos positivos pode ajudar a validar qual ataque confunde o controlador ao indicar que nós não maliciosos estão causando ataques no controlador.

7 REFERÊNCIAS

[1].TOLEDO, Cézar Murilo Geronaso de. Secure IT-SDN : a secure implementation of software defined wireless sensor network [doi:10.11606/D.3.2020.tde-11012022-120120]. São Paulo : Escola Politécnica, Universidade de São Paulo, 2020. Dissertação de Mestrado em Sistemas Digitais. [acesso 2023-11-30].

[2].ALVES, Renan Cerqueira Afonso. Achieving efficient routing in constrained networks with unidirectional links through Software Defined Networking. 2020. Tese (Doutorado em Sistemas Digitais) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2020. doi:10.11606/T.3.2020.tde-17122020-103717. Acesso em: 2023-11-30.

[3].M. Rahouti, K. Xiong, Y. Xin, S. K. Jagatheesaperumal, M. Ayyash and M. Shaheed, "SDN Security Review: Threat Taxonomy, Implications, and Open Challenges,"in IEEE Access, vol. 10, pp. 45820-45854, 2022, doi: 10.1109/ACCESS.2022.3168972

[4].NUNEZ SEGURA, Gustavo Alonso. Cooperative intrusion detection for software-defined resource-constrained networks. 2022. Tese (Doutorado em Sistemas Digitais) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.3.2021.tde-22022022-093544. Acesso em: 2023-11-30.

[5]. WOOLDRIDGE, M. An introduction to multiagent systems. [S.l.: s.n.]: John wiley and sons, 2009.

[6] SEGURA, Gustavo A. Nunez; CHORTI, Arsenia; MARGI, Cíntia Borges. IDIT-SDN: Intrusion Detection Framework for Software-defined Wireless Sensor Networks. In: SALÃO DE FERRAMENTAS - SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS (SBRC), 41. , 2023, Brasília/DF. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2023 . p. 56-63. ISSN 2177-9384. DOI:.

[7] https://github.com/renzoabensur/IDIT-SDN-Asymmetric-Link

[8] ALVES, R. C.; OLIVEIRA, D. A.; NÚÑEZ, G. A.; MARGI, C. B. It-sdn: Improved

architecture for sdwsn. XXXV Simpósio Brasileiro de Redes de Computadores, 2017.