



**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO
GRANDE DO NORTE**

ANDREZA DA SILVA VITAL

JEFFERSON CYPRIANO MONTEIRO VIEIRA

**UMA ANÁLISE DE DESEMPENHO E SEGURANÇA NAS REDES DEFINIDAS
POR SOFTWARE**

Canguaretama, RN – 2017

ANDREZA DA SILVA VITAL

JEFFERSON CYPRIANO MONTEIRO VIEIRA

**UMA ANÁLISE DE DESEMPENHO E SEGURANÇA NAS REDES DEFINIDAS
POR SOFTWARE**

(Ficha Catalográfica no verso, Biblioteca responsável pela elaboração)

Trabalho de Conclusão de Curso apresentado ao Curso Técnico em Informática do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, em cumprimento às exigências legais como requisito parcial à obtenção do título de Técnico em Informática.

Orientador: Prof. M.e. Helber Wagner da Silva

CANGUARETAMA/RN

2017

ANDREZA DA SILVA VITAL
JEFFERSON CYPRIANO MONTEIRO VIEIRA

**UMA ANÁLISE DE DESEMPENHO E SEGURANÇA NAS REDES DEFINIDAS POR
SOFTWARE**

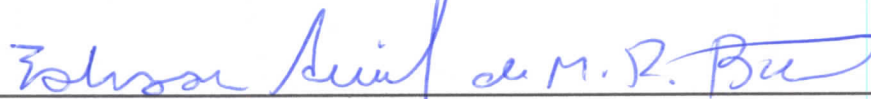
Trabalho de Conclusão de Curso apresentado ao Curso Técnico em Informática do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, em cumprimento às exigências legais como requisito parcial à obtenção do título de Técnico em Informática.

Aprovado em: 27/12/2017

Banca Examinadora



Prof. M.e. Helber Wagner da Silva - Presidente
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte



Prof. M.e. Edson Aníbal de Macedo Reis Batista - Examinador
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte



Prof. Dr. Éberton da Silva Marinho - Examinador
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

RESUMO

As Redes Definidas por *Software* (do inglês, *Software Defined Networks* - SDN) têm sido consideradas infraestruturas viáveis para suportar uma vasta diversidade de aplicações emergentes, como o transporte inteligente autônomo, videovigilância inteligente, vídeo sob demanda, redes elétricas inteligentes dentre outras aplicações graças à (re)programabilidade dinâmica, via *software*, dos serviços da rede. Entretanto, a SDN apresenta vulnerabilidades no plano de controle centralizado e no protocolo de sinalização com o plano de dados, podendo se tornar assim alvo de ataques por parte de usuários maliciosos. Com base nessa problemática, este relatório apresenta uma taxonomia, constituída com os principais ataques direcionados às vulnerabilidades da SDN e os mecanismos de segurança encontrados como forma de minimizar o impacto provenientes de tais ataques. O principal objetivo da taxonomia proposta é guiar futuros estudos mais aprofundados sobre a segurança em SDN.

Palavras-chaves: Redes Definidas por *Software*, Taxonomia, Ataques, Mecanismos de Segurança.

LISTA DE ILUSTRAÇÕES

| | |
|---|----|
| FIGURA 1. TOPOLOGIA DA REDE SIMULADA | 20 |
| FIGURA 2. TAXA DE PERDA DE PACOTE COM A VARIAÇÃO DA PROBABILIDADE DE DESCARTES DE ATACANTES | 22 |

LISTA DE TABELAS

| | |
|---|----|
| TABELA 1. ATAQUES E PARÂMETROS DO AMBIENTE DE SIMULAÇÃO | 21 |
| TABELA 2. ATAQUES E DEFESAS EM REDES SDN | 24 |

SUMÁRIO

| | |
|--|----|
| 1. INTRODUÇÃO | 8 |
| 2. REFERENCIAL TEÓRICO | 10 |
| 2.1 REDES DE COMPUTADORES | 10 |
| 2.1.1 PROTOCOLO IP | 11 |
| 2.2 REDES DEFINIDAS POR SOFTWARE | 12 |
| 2.3 ATAQUES | 12 |
| 2.4 MECANISMOS DE DEFESA | 15 |
| 2.4.1 SISTEMAS DE DETECÇÃO DE INTRUSÃO (IDS) | 15 |
| 2.4.1.1 HOST BASED INTRUSION DETECTION SYSTEMS (HIDS) | 16 |
| 2.4.1.2 NETWORK BASED INTRUSION DETECTION SYSTEMS | 16 |
| 2.4.1.3 IDS BASEADO EM ASSINATURAS | 17 |
| 2.4.1.4 IDS BASEADO EM ANOMALIAS | 17 |
| 3. METODOLOGIA | 19 |
| 4. ANÁLISE DE DADOS | 20 |
| 4.1 UMA ANÁLISE DOS ATAQUES DE ENCAMINHAMENTO EM REDES DEFINIDAS POR SOFTWARE | 20 |
| 4.2 UMA TAXONOMIA DOS MECANISMOS DE SEGURANÇA EM REDES DEFINIDAS POR SOFTWARE | 23 |
| CONSIDERAÇÕES FINAIS | 26 |
| REFERÊNCIAS | 27 |

1. INTRODUÇÃO

As Redes Definidas por Software (do inglês, *Software Defined Networks* - SDN), um novo paradigma de redes de comunicação de dados, surgem como uma solução para o problema encontrado para o desenvolvimento de aplicações inteligentes por permitir um controle dinâmico e adaptável dos recursos de redes. Na SDN, por meio da separação entre o plano de controle (que define as políticas de encaminhamento de pacotes) e o plano de dados (que efetivamente transmite os pacotes), facilita-se o gerenciamento dos serviços de rede, como o roteamento. Essas redes incluem um elemento onde o plano de controle é centralizado, chamado Controlador, que pode definir políticas de encaminhamento dos dados e (re)definir serviços de rede dinamicamente (BOUCADAIR, 2014). Atualmente, as SDNs têm sido consideradas infraestruturas viáveis para suportar aplicações inteligentes, inclusive na Internet das Coisas (do inglês, *Internet of Things* - IoT). Ainda assim, tais redes possuem vulnerabilidades no plano de controle centralizado e no seu protocolo de comunicação (OpenFlow), que podem ser exploradas por ataques (ex., os de encaminhamento de dados, envenenamento de rotas, dentre outros), visando provocar o mau funcionamento da rede ou até mesmo negar serviços de rede.

Entretanto, as redes de comunicação de dados tradicionais (IP) são limitadas em termos de gerenciamento dinâmico de recursos de rede, o que representa um obstáculo para o desenvolvimento de aplicações inteligentes, já que as mudanças de configuração dos elementos de rede, como *switches* e roteadores, ou a inclusão de novas funcionalidades dependem do fabricante e, essa dependência pode resultar em procedimentos demorados e de alto custo. Desse modo, as aplicações emergentes necessitam de um novo paradigma de redes de comunicação de dados, capaz de resolver as limitações encontradas nas redes tradicionais, ou seja, uma rede adaptável, flexível e gerenciável.

Este relatório apresenta uma classificação dos ataques encontrados e dos mecanismos de segurança que buscam prevenir, identificar e isolar ameaças de

rede nas SDN. Além disso, analisamos o impacto de ataques direcionados às SDN no desempenho das aplicações.

2. REFERENCIAL TEÓRICO

Esta seção apresenta o embasamento teórico necessário para o entendimento da taxonomia de ataques e mecanismos de segurança em Redes Definidas por *Software* (SDN) descrita neste relatório. Revisada uma literatura recente (2011 em diante), artigos científicos publicados em eventos e periódicos relevantes na área de segurança em redes de comunicação de dados.

2.1. REDES DE COMPUTADORES

Uma rede de computadores é um conjunto de um ou mais computadores interconectados entre si para a troca de dados (p. ex., arquivos, mensagens e etc.) e compartilhamento de recursos (p. ex., processamento, armazenamento e etc.). A Internet representando uma rede de computadores em escala mundial, dando o suporte a aplicações de rede, como correios eletrônicos, comércios eletrônicos, redes sociais virtuais, dentre outros, que foi concebida de acordo com um modelo em camadas, chamado modelo TCP/IP (KUROSE, 2010).

O modelo TCP/IP define a rede em 5 (cinco) camadas: Aplicação, Transporte, Rede, Enlace e Física. Cada uma das camadas oferecendo serviços como transporte confiável de dados, endereçamento de máquinas, controle de acesso aos equipamentos, dentre outros, existindo formas de interação entre eles que ocorrem de acordo com protocolos de rede. Um protocolo de rede define o formato e a ordem das mensagens (isto é, um conjunto de bits bem definido) trocadas entre dois ou mais sistemas finais (programas). Além disso, o protocolo especifica as ações realizadas na transmissão e/ou no recebimento de uma mensagem.

Cada camada da rede possui um conjunto de protocolos que permitem as comunicações entre sistemas finais em execução em diferentes hospedeiros. O serviço da Camada Física é movimentar os bits individuais de um nó (computador, switch, roteador, etc.) para outro, através de um enlace, que conecta uma placa de rede a outra. O serviço da Camada de Enlace é responsável por controlar o acesso dos bits ao enlace, buscando evitar colisões (interferências) que provocam a perda de bits colididos. A Camada de Rede tem o objetivo principal de estabelecer rotas

através das quais os bits são transmitidos de um nó a outro da rede. A Camada de Transporte controla o envio e a entrega de informações aos sistemas finais, e por fim, na Camada de Aplicação são executadas as aplicações de rede.

Podemos destacar dois serviços principais que a camada de redes oferece à Camada de Transporte no modelo TCP/IP, sendo estes o repasse e o roteamento. O serviço de repasse envolve a transferência de um conjunto de bits (chamado de pacote) de uma interface de rede para outra em um mesmo equipamento (p. ex., roteador). Já o serviço de roteamento determina o caminho (isto é, a sequência de nós e enlaces) através do qual os pacotes são enviados, desde o nó origem até o nó destino. Como principal protocolo da Camada de Rede está o Internet Protocol (IP).

2.1.1. PROTOCOLO IP

O protocolo IP é um importante conjunto de regras que suportam o endereçamento de equipamentos, como roteadores e computadores, e os serviços de repasse e roteamento através da infraestrutura de rede. Atualmente, existindo duas versões do protocolo IP, chamadas de IPv4 e IPv6, que coexistem entre si. O protocolo IPv4 define um endereço, chamado endereço IP, para cada interface de rede (p. ex., em um roteador). Este sendo representado por um conjunto de 32 bits, o que permite portanto espaço de endereçamento de 2³² endereços IP diferentes. Sua escrita é em notação decimal separada por pontos (*dotted-decimal notation*), como 10.0.0.1, 192.168.0.1.

No IPv4, um pacote (também denominado datagrama) pode ser fragmentado (isto é, dividido) em dois ou mais datagramas IP menores, considerando a capacidade de transmissão de um enlace. Nesse caso, os diferentes datagramas podem ser enviados através de diferentes rotas entre a fonte e o destino, considerando as decisões do protocolo de roteamento em execução nos roteadores. A abordagem de fragmentação no IPv4 possui vulnerabilidades. Em primeiro lugar, ela aumenta a complexidade do projeto de roteadores e sistemas finais, que precisam ser projetados para acomodar a fragmentação do datagrama e o reagrupamento. E, em segundo lugar, a fragmentação pode ser alvo de ataques do

tipo Negação de Serviço (do inglês, Denial of Service - DoS), em que um atacante pode enviar uma sequência de fragmentos inesperados.

2.2. REDES DEFINIDAS POR SOFTWARE

O trabalho de Guedes et. al (2012) apresenta as Redes Definidas por Software (do inglês, Software Defined Networking - SDN), como uma abordagem recente na administração de redes de comunicação. Na SDN, há uma separação entre os planos de controle (que definem políticas de encaminhamento de pacotes) e de dados (que efetivamente transmitem pacotes) que facilita o gerenciamento dos serviços de rede, como roteamento. Os principais componentes de uma SDN são o Controlador SDN e os comutadores.

O Controlador SDN é um *software* que atua como um sistema operacional de rede. Ele provê o controle direto dos comutadores da rede, que efetivamente repassam pacotes entre si. Para tanto, o controlador SDN envia mensagens de sinalização que instalam regras e ações de repasse nos computadores da rede. A comunicação entre um controlador SDN e os comutadores ocorre através de mensagens de protocolos, como OpenFlow, NETConf, etc. O OpenFlow sendo considerado o principal protocolo de comunicação nas SDNs, permitindo que equipamentos de rede comerciais e convencionais possam interagir entre si.

2.3. ATAQUES

O trabalho de Silva (2011) apresenta conceitos relacionados aos ataques em redes de comunicação de dados. Tais ataques buscam explorar vulnerabilidades encontradas na rede a fim de provocar mau funcionamento de serviços, como o roteamento, o que reduziria o desempenho da rede na entrega de pacotes de dados. Chamamos o agente responsável por lançar o ataque de *atacante*, que pode ser um humano, um sistema ou um equipamento de rede, por exemplo, um roteador ou switch.

Quanto ao modo de atuação, podemos definir os ataques como passivos e ativos. No primeiro, os atacantes buscam obter dados privados dos usuários no meio sem fio, enquanto operam normalmente nos serviços de rede. Já no segundo, os atacantes executam ações maliciosas, como a fabricação, a modificação e o descarte de dados, para comprometer o funcionamento correto dos serviços ou até mesmo negá-los. Além disso, os ataques podem ser classificados de acordo com a camada da pilha de protocolos onde atuam. Por exemplo, na camada de rede temos os ataques de fabricação, modificação, tunelamento, descarte seletivo e buraco negro.

No ataque de fabricação de pacotes, o atacante lança falsos pacotes de controle de descoberta de rotas e de notificação de quebra de enlaces, podendo resultar no isolamento de nós legítimos e na configuração de rotas inexistentes. Ao passo que no ataque de modificação de pacotes, o nó malicioso altera as informações armazenadas nos pacotes de controle usados pelo protocolo de roteamento. No ataque de tunelamento (*wormhole*), uma conexão é estabelecida entre dois nós atacantes distantes um do outro usando um enlace com baixa latência (túnel). Assim, quando os atacantes conseguem participar de uma rota, eles podem analisar o tráfego de dados privados dos usuários ou desviar os pacotes de controle do roteamento. No ataque de descarte seletivo de pacotes, o atacante usa uma distribuição probabilística para descartar os pacotes de dados enviados por nós legítimos. Já no de descarte de pacotes, o nó malicioso descarta todos os pacotes enviados pelos nós legítimos.

Assim como as redes tradicionais, as redes SDN também têm sido alvo de diferentes ameaças que buscam explorar suas vulnerabilidades e prejudicar os serviços de rede para, conseqüente, reduzir o desempenho das aplicações. O trabalho de Kloti et. al (2013) apresenta uma análise de segurança da rede OpenFlow utilizando o método STRIDE. Com base nos resultados obtidos, os autores destacam quais os ataques aos quais a rede é vulnerável, são eles: Negação de Serviço (DoS), Divulgação de Informação e Adulteração. O trabalho também aponta algumas estratégias para os ataques DoS, que podem ser: Limitação de taxa, filtragem de pacotes, *Packet Dropping* e Ajustamento *Timeout*. Na

verdade, detectar ataques do tipo DoS é um problema muito difícil e uma área em aberto.

Já o trabalho de Scott-Haymard et. al (2013) mostra que as vantagens da rede podem levar às vulnerabilidades de segurança. No trabalho, uma tabela inclui referenciais de segurança e mecanismos de defesa e outra abrange o mapeamento dos ataques na rede SDN, tratando em especial as vulnerabilidades dos planos de controle e de dados. Os autores discutem a implementação de uma camada adicional, que fica entre o controlador e os dispositivos de rede, para interceptar possíveis problemas. Recentemente, tem havido uma discussão sobre a integração de middle-boxes na rede para fornecer funções de segurança.

O trabalho de Kandoi et. al (2015) aborda dois tipos de ataque DoS. Um deles ataca a largura de banda do plano de controle e o outro a tabela de fluxo do *switch*. No primeiro, sempre que o *switch* recebe um pacote que não está em sua tabela de fluxo ele guarda o pacote e envia uma mensagem OFTP_PACKET_IN ao controlador, entanto, quando o *buffer* do switch está cheio, é necessário que todo o pacote seja enviado ao controlador. Nesse caso, a resposta não contém uma regra de fluxo, então aquele pacote, caso seja enviado várias vezes, precisará ser encaminhado ao controlador deixando lento o tráfego da rede. O segundo tipo de ataque explora a limitação da quantidade de entradas na tabela de fluxo do switch. Ao receber uma mensagem FLOW_MOD, se o switch constata que sua tabela está cheia, ele envia uma mensagem OFTP_ERROR ao controlador, ficando incapaz de avançar até o problema ser contornado pelo controlador. Este é um ataque local, levando em consideração que não afeta toda a rede e sim o switch que recebeu o pacote.

O trabalho de THANH BUI (2015) trata de ataques de envenenamento de topologia, que consiste em alterações maliciosas em tabelas de roteamento ou repasse para direcionar pacotes de dados para outros hospedeiros (*hosts*) maliciosos em vez de direcionar para os hosts apropriados. Imagine a seguinte situação: o dispositivo A na rede A deseja se comunicar com o dispositivo B na rede B. Estas duas redes estão conectadas por um dispositivo roteador. E neste roteador

há uma tabela de roteamento que irá indicar por qual interface a mensagem será encaminhada para que consiga chegar ao seu destino. Mas se a rede tiver sofrido um ataque de envenenamento de topologia, as portas podem estar erradas e, conseqüentemente, serem encaminhadas para um dispositivo malicioso C.

Ainda no trabalho de THANH BUI (2015) três cenários diferentes de ataques são apresentados: Two-switch tunnel, Extended two-switch tunnel e Single-switch tunnel. O objetivo do primeiro ataque é levar o controlador a acreditar que os switches comprometidos estão diretamente ligados, do segundo é levar o controlador a acreditar que os switches comprometidos estão diretamente ligados e por isso são seus vizinhos e do terceiro é levar o controlador a acreditar que os vizinhos do switch comprometido estão diretamente ligados um ao outro.

2.4. MECANISMOS DE DEFESA

A criação de redes SDN seguras é uma área recente de pesquisa científica no âmbito das redes de computadores (BENTON, 2013). O trabalho de SILVA (2011) apresenta noções sobre os principais mecanismos de segurança contra os ataques em SDN. Em linhas gerais, podemos classificar os mecanismos de segurança em preventivos ou reativos, de acordo com o nível de comprometimento da rede. Os mecanismos preventivos buscam impedir a entrada de atacantes na rede de comunicação, como exemplos de mecanismos preventivos podemos incluir a criptografia e os *firewalls*. Já os mecanismos de segurança reativos (sobretudo os sistemas de detecção de intrusão) tentam identificar e isolar os atacantes que conseguiram invadir a rede, superando os mecanismos preventivos.

2.4.1. SISTEMAS DE DETECÇÃO DE INTRUSÃO (IDS)

O trabalho de NAGAHAMA (2013) apresenta informações técnicas sobre os Sistemas de Detecção de Intrusão (do inglês, Intrusion Detection Systems - IDS), classificados como mecanismos de defesa reativos. Os IDSs representam sistemas que monitoram eventos e analisam anomalias de intrusão em sistemas

computacionais, detectando atividades maliciosas ou anômalas, alertando o administrador do sistema que esses eventos estão ocorrendo. Eles podem ser classificados basicamente de acordo com o local de atuação e com o tipo de técnica utilizada para análise conforme os seguintes aspectos; quanto ao local de atuação, o IDS pode ser baseado em *host* ou baseados na rede; á quanto à técnica de análise, o IDS pode ser baseado em: em assinatura, em anomalia ou híbrida.

2.4.1.1. HOST BASED INTRUSION DETECTION SYSTEMS (HIDS)

Nos IDSs baseados em *host*, os monitores são instalados em um *host* e sua atuação tem como objetivo analisar as informações contidas na própria máquina. Aspectos internos, como processos em execução, alterações não autorizadas em arquivos, instalação de executáveis, alterações de registros, verificação da integridade de executáveis, envio de tráfego na rede, entre outros, são informações monitoradas pelos HIDS. Como algumas vantagens estão detectar ataques em eventos locais que poderiam ser detectados pela rede; analisar dados criptografados; e não serem limitados pelo uso de switches na rede sem o recurso de espelhamento de portas. Como desvantagens, por exemplo, podemos citar; a difícil instalação e manutenção; a fácil detecção pelo invasor; a limitada detecção de ataques de rede; e a redução no desempenho do funcionamento do host.

2.4.1.2. NETWORK BASED INTRUSION DETECTION SYSTEMS (NIDS)

Nos NIDS baseados em rede, o monitor é instalado na rede e suas(s) interface(s) de rede atua(m) em um modo especial denominado de “modo promíscuo”, podendo capturar (isto é, verificar) o tráfego de rede em tempo real e analisando os pacotes que estão trafegando na rede, mesmo estes sendo destinados para o próprio monitor. Possuem algumas vantagens, como serem transparentes para o atacante; serem de fácil implantação; não interferirem no desempenho dos hosts e serem independentes de plataforma. Como desvantagens

podemos citar a dificuldade em tratar dados de rede de alta velocidade, a adição de retardos nos pacotes e a dificuldade em manipular dados criptografados.

Quanto ao local de atuação na rede, os NIDSs podem ser classificados em ativos ou passivos. Os ativos são instalados em um ponto para interceptar o tráfego de rede, de forma semelhante a uma ponte (bridge), e analisar o tráfego passante, com isso se torna capaz de bloquear um tráfego caracterizado como malicioso ou indevido. Porém, um subdimensionamento do hardware utilizado pode adicionar retardos excessivos aos pacotes, podendo degradar o desempenho da rede. Os de modo passivo analisam apenas cópias dos pacotes da rede que atravessam o switch ou hub onde está sendo executado. Devido à heterogeneidade de fabricantes e modelos de equipamentos utilizados em uma rede, sem uma integração com outro equipamento de rede, que normalmente devem ser da mesma solução e/ou fabricante, a ação de um NIDS passivo fica limitada a apenas notificar a detecção de um tráfego malicioso.

2.4.1.3. IDS BASEADO EM ASSINATURAS

O IDS baseado na técnica de assinaturas analisa o tráfego da rede considerando uma base de assinaturas de ataques com padrões previamente conhecidos e catalogados. Como vantagem, tem o pouco consumo de recursos e o rápido processamento, mas, como desvantagem, exige constantes atualizações da base de assinaturas, tem um alto índice de falsos positivos e exigem um bom nível de conhecimento na geração da base.

2.4.1.4. IDS BASEADO EM ANOMALIAS

Já os IDSs baseados na técnica de anomalias comparam o comportamento atual da rede com o comportamento previamente registrado como normal na fase de aprendizagem, e alertam quando ocorre um desvio nos padrões de tráfego de rede. Como vantagem está a detecção de novos ataques através do desvio de comportamento sem a necessidade de conhecer detalhadamente a intrusão. A sua desvantagem se relaciona com a possibilidade de gerar grande número de falsos

alertas em decorrência de modificações no comportamento do host ou da rede, mesmo não se tratando de um tráfego malicioso; e o extensivo processo para a geração do perfil de comportamento considerado normal. Por fim, os IDSs baseados na técnica híbrida combinam diferentes classificadores, apresentando bons índices de detecção e baixa taxa de falsos positivos.

No artigo “A Framework for Security Services based on Software-Defined Networking” (Jaehoon (Paul) Jeong et. al, 2015), os autores analisam dois serviços de segurança representativos. O sistema de *firewall* centralizado e o Sistema de Mitigação ataque DDoS Centralizado. Em um sistema de firewall centralizado, o gerenciamento pode ser feito de forma flexível por um servidor centralizado. Ou seja, existe um controle de cada switch e as regras de firewall podem ser adicionadas ou excluídas dinamicamente. Um sistema de mitigação ataque DDoS pode adicionar, excluir ou modificar regras para cada roteador, defendendo servidores contra ataques DDoS fora da rede privada, ou seja, a partir da rede pública.

3. METODOLOGIA

Como metodologia para o desenvolvimento do projeto de pesquisa, que se desenvolveu entre 20/07/2015 à 31/03/2016, realizou-se um levantamento bibliográfico de artigos científicos direcionados à área de segurança em redes de comunicação de dados. Desta forma, estabeleceram-se metas a serem cumpridas, dispostas da seguinte maneira:

Meta 1 - 20/07/15 até 31/08/15

Elaboração de relatório técnico parcial sobre fundamentação teórica incluindo os principais conceitos sobre Redes de Computadores, Redes SDN, Ataques e Mecanismos de Segurança em redes de comunicação de dados.

Meta 2 - 01/09/15 até 30/11/15

Elaboração de um relatório técnico parcial, incluindo a atividade de revisão de literatura recente (2012-2015) sobre os principais ataques direcionados às redes SDN.

Elaboração de um relatório técnico parcial, incluindo a atividade de revisão de literatura recente (2012-2015) sobre os principais mecanismos de segurança e seus requisitos para aplicação às redes SDN.

Meta 3 - 01/12/15 até 31/03/16

Elaboração de artigo científico modelo CONNEPI, contendo as especificações dos desafios de segurança e desempenho em redes SDN para viabilizar novos projetos de pesquisadores e profissionais na área de Redes de Comunicação de Dados para a IoT.

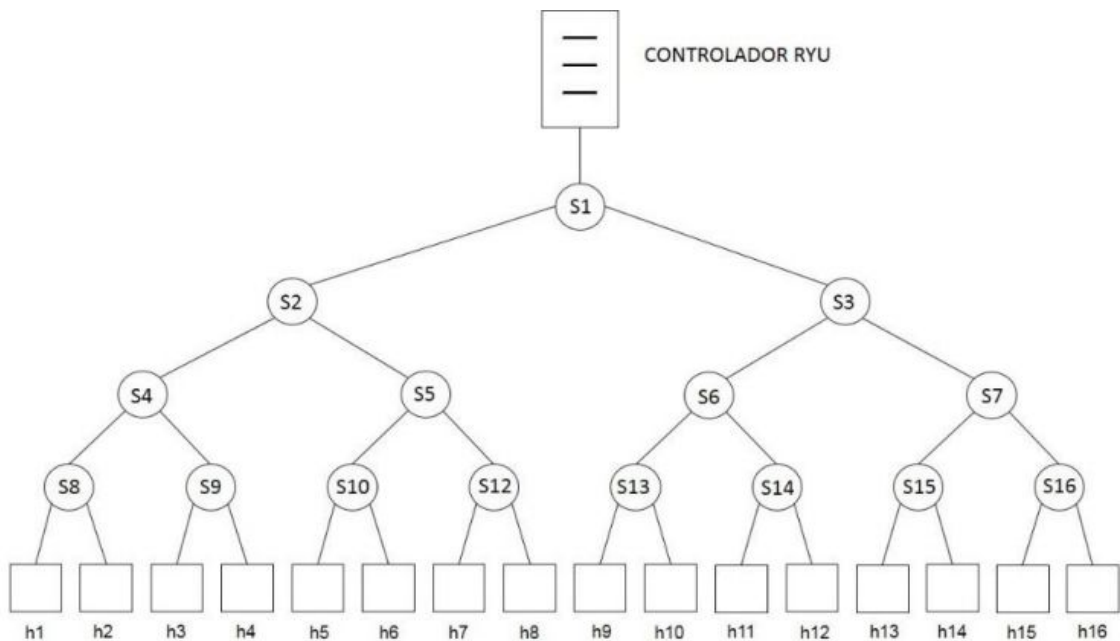
Além de uma revisão literária, realizou-se simulações de rede com o objetivo de analisar o impacto que um ataque de encaminhamento de dados exerceria em uma rede SDN. Os resultados serão apresentados de forma detalhada na seção seguinte.

4. ANÁLISE DE DADOS

4.1. UMA ANÁLISE DOS ATAQUES DE ENCAMINHAMENTO EM REDES DEFINIDAS POR SOFTWARE

Através de simulação, usando o simulador de rede Mininet, se analisou o impacto de ataques direcionados às SDN no desempenho das aplicações. A Figura 1 descreve a topologia da rede simulada.

Figura 1 - Topologia da rede simulada



A implementação do ataque ocorre da seguinte forma. Quando o switch encaminha uma mensagem do tipo PACKET_IN para o Controlador Ryu (baseado em Python), este calcula um valor aleatório (x) e o compara com o valor da probabilidade de descarte (p) previamente definida (variando de 0.0 a 1.0). Se o valor de x for maior ou igual ao valor de p , então o controlador envia uma mensagem FLOW_MOD para o switch instalando uma regra sem nenhuma action. Uma regra sem action indica que o switch descarta qualquer pacote de dados recebido e, em outras palavras, executa o ataque. Caso o valor de x seja menor que p , então a mensagem FLOW_MOD é enviada com a regra contendo uma action (e.g., output) apropriada ao fluxo de dados. Isso significa que o switch encaminhará o pacote de dados normalmente, ou seja, sem lançar ataques.

Para avaliar o impacto dos ataques, consideramos duas métricas significativas para medir o desempenho de uma rede: a Taxa de Perda de Pacotes (TPP) e o *jitter*. A TPP significa a razão entre a quantidade de pacotes efetivamente recebidos pelo destino e a quantidade de pacotes enviados pela fonte. Essa métrica é relevante porque diferentes aplicações, por exemplo, de vídeo, possuem requisitos de Qualidade de (GEORGOPOULOS, 2013) Serviço (do inglês, Quality of Service - QoS) e requerem TPP de, no máximo, 1% . Por sua vez, o *jitter*, medido em milissegundos (ms), significa a variação da latência, que é o tempo que um pacote leva para sair da fonte até chegar ao destino. Cada ponto plotado nos gráficos de resultados representa o valor médio de 5 rodadas de simulação. A Tabela 1 descreve todos os parâmetros usados nas simulações.

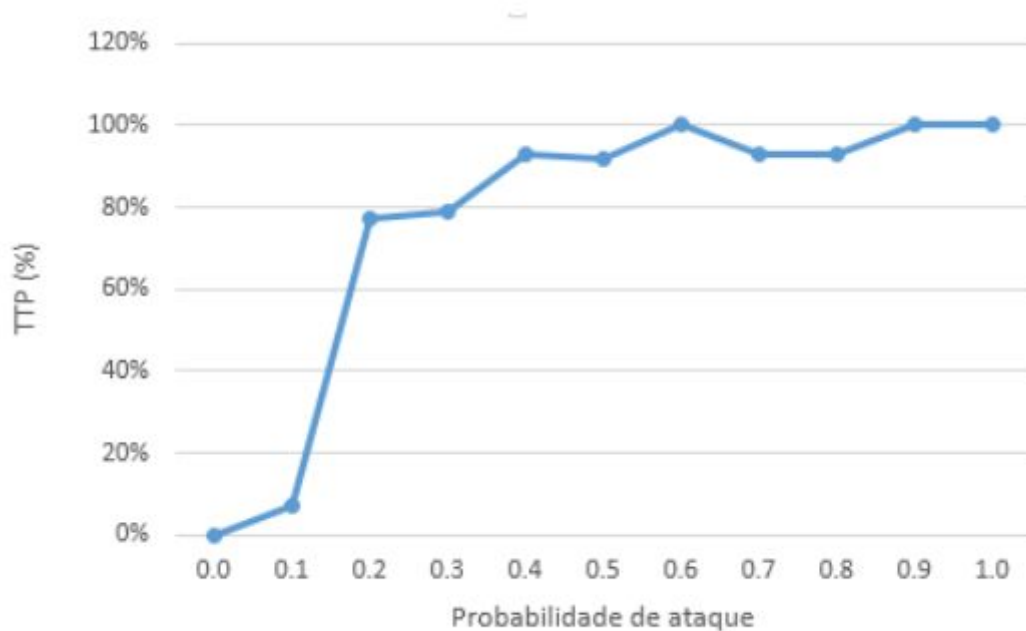
Tabela 1 - Parâmetros do ambiente de simulação

| Parâmetro | Descrição |
|---|--|
| Topologia da rede | Árvore binária |
| Quantidade de <i>switches</i> | 16 |
| Quantidade de <i>hosts</i> | 16 |
| Controlador SDN | Ryu |
| Largura de banda dos enlaces | 10Mbps |
| Ferramenta geradora de tráfego de dados | Iperf |
| Padrão de tráfego | Taxa de 4Mbps segundo padrão CBR (<i>Constant Bit Ratio</i>) |
| Tempo de simulação (segundos) | 20s |
| Taxa de descarte de pacotes pelos nós atacantes | Variável, entre 0.0 e 1.0 |

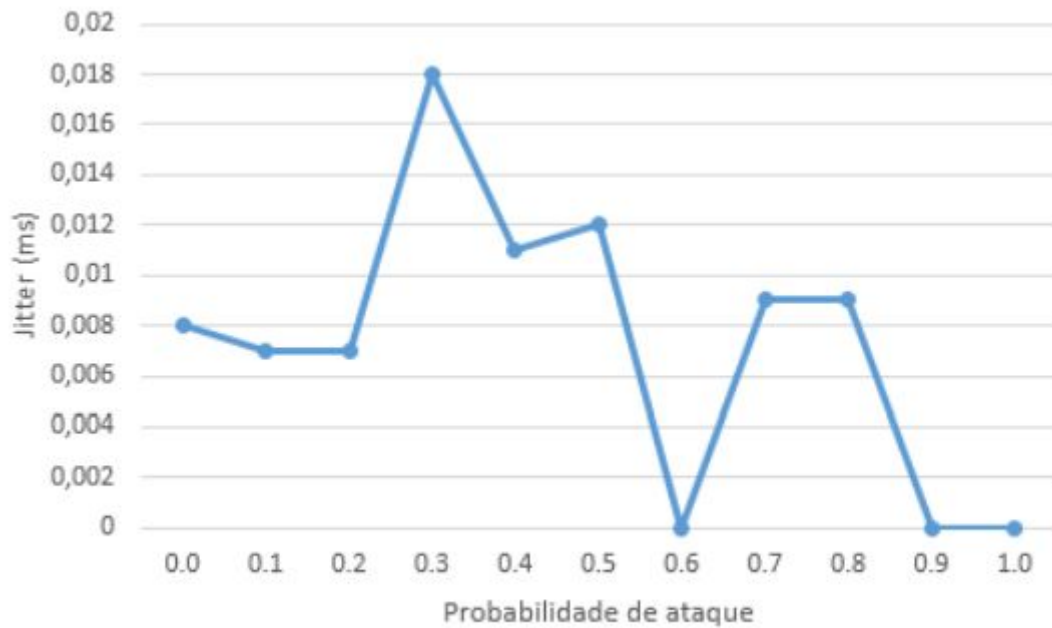
A Figura 2 mostra os resultados do valor TPP com o aumento da probabilidade de descarte (p) de dados pelos atacantes. Pode-se observar que o aumento da probabilidade de ataques provoca o crescimento significativo da TPP, independentemente do valor de p . Quando o valor de p está entre 0.0 e 0.1 (o que representa uma menor probabilidade de ataque), observa-se um aumento de 7% na TPP. Entretanto, quando p atinge o valor 0.2, a TPP apresenta um aumento para 77%. Em outras palavras, apenas uma média de 23% dos pacotes enviados pela fonte efetivamente são recebidos pelos destinatários. Quando p possui valor 1.0 (i.e.,

alta probabilidade de ataque), o valor da TPP é de 100% e todos os pacotes são descartados pelos atacantes.

Figura 2 - Taxa de Perda de Pacotes com a variação da probabilidade de descarte dos atacantes



A Figura 3 apresenta os valores do *jitter* diante do crescimento do valor da probabilidade p de descarte nos atacantes. Os resultados obtidos mostram que não há um crescimento do *jitter* associado necessariamente com o aumento de p . Observa-se, no entanto, que quando o valor de p tende a 1.0, o valor do *jitter* também tende a 0 porque não há troca de mensagens e, portanto, não é possível mensurar essa métrica.

Figura 3 - *Jitter* com a variação da probabilidade de descarte dos atacantes

4.2. UMA TAXONOMIA DOS MECANISMOS DE SEGURANÇA EM REDES DEFINIDAS POR SOFTWARE

A Tabela 2, representa um diagnóstico dos estudos realizados acerca dos ataques direcionados a SDN e os meios de defesa encontrados com o intuito de minimizar os resultados causados à rede caso esta seja alvo destes ataques.

Tabela 2. Ataques e Defesas em redes SDN.

| Ataque | IDS | Criptografia | Autenticação | Limitação da Taxa | Filtragem de Eventos |
|----------------------------|-----|--------------|--------------|-------------------|----------------------|
| Negação de Serviço | | | | X | X |
| Envenenamento de topologia | X | X | X | | |
| <i>Man in the Middle</i> | X | X | X | | |
| Adulteração de Pacotes | X | X | X | | |

Fonte: do próprio autor.

Os IDSs podem detectar ataques (NAGAHAMA, 2013), como os de Envenenamento de Topologia, *Man in the Middle* e os de Adulteração de Pacotes. Os IDSs são classificados como reativos ao ataque. No entanto, não conseguem detectar ataques com tráfegos agressivos. Já a Criptografia e a Autenticação podem evitar os ataques de Envenenamento de Topologia, *Man in the Middle* e Adulteração de Pacotes, garantindo que apenas o destinatário desejado tenha acesso a informação. Por sua vez, a Limitação de Taxa e a Filtragem de Eventos são estratégias contra os ataques de Negação de Serviço e os de Negação de Serviço Distribuído.

Para o desenvolvimento de projetos arquitetônicos que desenvolvem aplicações de segurança utilizando SDN e rede de monitorização, são trabalhados requisitos como: A replicação de controladores, tendo vários controladores em uma única rede, existe um aumento de confiabilidade e tolerância a falhas. Isto podendo ser conseguido com a migração de funcionalidades, de um controlador falho para outro controlador que está em seu funcionamento. O SDN dissociar o plano de controle do plano de dados, no entanto, não dissociar as funcionalidades de controle de monitoramento. Por exemplo, uma OpenFlow seria responsável por comunicar as mensagens de controle para os roteadores e monitorar o tráfego na rede ao mesmo tempo, isto aumentando a sobrecarga no controlador, e, assim, diminuindo o seu rendimento.

Dentre outros, um requisito de uma arquitetura SDN flexível seria ter componentes fracamente acoplados, isto é, que não contam com a funcionalidade de cada um. Por exemplo, ao desenvolver uma aplicação, esta deve ser capaz de funcionar independentemente do tipo do controlador SDN a ser utilizado. E um requisito para a detecção de ataques de alta resolução seria a capacidade de um aplicativo de segurança funcionar independente da quantidade de informação que lhe é dado como entrada. Por exemplo, o OpenFlow fornece informações de baixo nível, com pacotes por fluxo, mas não provê informações sobre o nível de pacote (p. ex., comprimento do cabeçalho). Uma abordagem de detecção de ataques que

possui alta resolução fornece o máximo de informações possíveis sobre o tráfego da rede.

CONSIDERAÇÕES FINAIS

As redes SDN oferecem vantagens na (re)programação dinâmica dos serviços de rede via software diretamente nos dispositivos, tornando-as infraestruturas eficientes e escaláveis para suportar as aplicações inovativas da IoT. Entretanto, diferentes ataques têm explorado as vulnerabilidades de segurança do protocolo OpenFlow e do controlador centralizado para corromper ou até mesmo interromper serviços, como o encaminhamento de dados. Este relatório apresentou uma taxonomia que classifica os mecanismos de defesa que podem atuar contra determinados ataques direcionados a SDN, que se propõe a guiar futuros estudos sobre o cenário de segurança nas redes SDN.

REFERÊNCIAS

BENTON, Kevin; CAMP, L. Jean; SMALL, Chris. Openflow vulnerability assessment. In: Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, 2013. p. 151-152.

BOUCADAIR, Mohamed; JACQUENET, Christian. Software-defined networking: A perspective from within a service provider environment. 2014.

GUEDES, Dorgival, et al. "Redes Definidas por Software: uma abordagem sistêmica para o desenvolvimento de pesquisas em Redes de Computadores." Minicursos do Simpósio Brasileiro de Redes de Computadores-SBRC 2012 30.4 (2012): 160-210.

JEONG, Jaehoon Paul et al. A Framework for Security Services based on Software-Defined Networking, 2015.

KANDOI, Rajat; ANTIKAINEN, Markku. Denial-of-service attacks in OpenFlow SDN networks. In: Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on. IEEE, 2015. p. 1322-1326.

KLOTI, Rowan; KOTRONIS, Vasileios; SMITH, Paul. Openflow: A security analysis. In: Network Protocols (ICNP), 2013 21st IEEE International Conference on. IEEE, 2013. p. 1-6.

KUROSE, James F., and Keith W. Ross. "Redes de Computadores e a Internet", 5ª Edição. (2010)

NAGAHAMA, Fábio Yu. "IPSFlow: Um framework para Sistema de Prevenção de Intrusão baseado em Redes Definidas por Software." (2013).

SCOTT-HAYWARD, Sandra; O'CALLAGHAN, Gemma; SEZER, Sakir. Sdn security: A survey. In: Future Networks and Services (SDN4FNS), 2013 IEEE SDN For. IEEE, 2013. p. 1-7.

SILVA, Helber W. "Um esquema de seleção de rotas para o balanceamento de segurança e desempenho em Redes em Malha Sem Fio". Dissertação de Mestrado. (2011).

THANH BUI, Tien. Analysis of Topology Poisoning Attacks in Software-Defined Networking. 2015.

ZAALOUK, Adel et al. OrchSec: An orchestrator-based architecture for enhancing network-security using Network Monitoring and SDN Control functions. In: Network Operations and Management Symposium (NOMS), 2014 IEEE. IEEE, 2014. p. 1-9.