Redes Definidas por Software – SDN – Um estudo sobre as Vantagens e suas Características

Allan Christian M. Silva, Luiz Claudio G. Maia, Humberto F. Villela

Faculdade de Ciências Empresariais – Universidade FUMEC

Rua Cobre, 200 - 30.310-190 – Belo horizonte – MG – Brasil

christian.allan8@gmail.com, luiz.maia,humberto.villela@fumec.br

Resumo. As Redes Definidas por Softwares abrem uma nova perspectiva no controle lógico da rede com novas aplicações, desta forma suprem problemas encontrados nas redes tradicionais. Este estudo tem o objetivo de apresentar as principais vantagens das Redes Definidas por Software. Por meio de uma análise literária entre artigos científicos, foram avaliadas atualizações em hardwares, softwares é protocolos da arquitetura descrita. Entre os resultados obtidos e possível perceber que esse novo paradigma possibilita um melhor gerenciamento no tráfego e controle de dados, além de possibilitar estudos e experimentações sem grandes complicações a fim de obter novos recursos para a área.

Abstract. *Software Defined Networks open a New Perspective on the New Digital Network System. This study aims to present as main advantages of Software Defined Networks. By means of a literary analysis in scientific articles, the updates on hardware, software and protocols of the described architecture were evaluated. Among the results that can be realized, the new paradigm allows a better management without data control, besides making possible the studies realization and experiments in large quantities to obtain new resources for an area.*

1. Introdução

Estimativas apontam um crescimento de cerca de 1.114% entre os últimos anos no uso da internet global de acordo com *a Internet World Stats* (2019). Segundo Comer (2016, p.3) "a partir dos anos 1970, a comunicação via computador transformou-se em uma parte essencial de nossa infraestrutura".

As redes são mecanismos essenciais para internet global, sem elas não seria possível conectar as pessoas e computadores a esse principal sistema de comunicação atual. "A internet não é de modo algum uma rede, mas sim um vasto conjunto de redes diferentes que utilizam certos protocolos comuns e fornecem determinados serviços comuns" (TANENBAUM, 2003, p.54).

Com avanço das redes de computadores, houve o surgimento de indústrias especializadas, trazendo para esse mercado uma série de softwares, serviços e principalmente hardwares, atendendo assim toda essa demanda de pequeno, médio e grande porte, para que seja

possível conexões cada vez mais robustas, dentro de empresas, instituições de ensino, residências. Segundo Guedes et al. (2012), existem ainda dificuldades em inserir novos recursos, devido aos hardwares existentes no mercado possuírem uma arquitetura fechada, tornando assim impossível trabalhar com os protocolos de gerenciamento existentes.

Pesquisas em comunicação de dados e redes buscam novas tecnologias para melhor precisão e velocidade no tráfego de dados, (Forouzan, 2009). Com o crescente volume de tráfego de dados entre as redes de computadores, existe a grande necessidade de torná-las cada vez mais escaláveis, com isso é de extrema importância a introdução de novas tecnologias para suprir a enorme infraestrutura e principalmente o gerenciamento destas redes. Com tal demanda, pesquisadores e profissionais em TI vem implementando o paradigma de Redes Definidas por Software, ou *Software Defined Networks* (SDN). Abrindo novas perspectivas no controle lógico da rede com novas aplicações, fugindo da arquitetura atual, (Costa, 2013). Ganhando uma performance na agilidade e mobilidade no gerenciamento das mesmas. A SDN e baseada em tecnologias abertas, que possibilitam o gerenciamento de toda rede por meio de softwares. Esse recurso se caracteriza pela separação entre o plano de dados e controle, com o uso de padrões abertos, tendo um controlador programável centralizado que fica responsável por gerenciar os pacotes recebidos e encaminhá-lo ao seu destino, de acordo com a programação estabelecida. Uma das ferramentas primordiais que tornaram possível tal feito, foi o OpenFlow com padrão aberto para a SDN, que possibilita o uso de novos protocolos sobre os dispositivos de redes comerciais, em paralelo com a operação de rede atual, (GUEDES et al, 2012).

Este estudo tem como objetivo identificar e analisar as principais vantagens na adoção das Redes Definidas por Software, serão avaliadas e comparadas as principais atualizações em hardwares, softwares e protocolos, e como essa tecnologia ajuda na implantação, gerenciamento, segurança e criações de pesquisa nas redes de computadores atuais.

Como toda nova tecnologia, é de extrema importância realizar um estudo a respeito da sua arquitetura e funcionamento. Desta forma pesquisas são essenciais para colocar em questão os motivos para construção e desenvolvimento de tal tecnologia e principalmente quais serão as vantagens que ela trará para o meio existente. Contribuindo assim para novas pesquisas e estudo entre estudantes e profissionais da área de Tecnologia da Informação (TI), pois mesmo com sua implantação existem ainda algumas áreas a serem exploradas. “Existem diversas oportunidades ainda em aberto para otimização no tráfego na rede através do uso de SDN ” (ANDRIOLI, ROSA RICHI e AUBIN,2017, p. 11).

2. Metodologia

Para construção deste artigo foi realizada uma revisão de literatura referente ao tema abordado.

Foi realizada uma análise entre as obras escolhidas, para o levantamento de informações pertinentes ao tema. Este estudo busca compreender as principais vantagens obtidas através de revisão de literatura. Dentre as vantagens algumas se destacam como:

i. Gerência de Redes
ii. Controle e Segurança
iii. Pesquisa e Experimentação

Na estratégia de busca, foram adotadas buscas manuais e principalmente automáticas em bibliotecas digitais, entre elas a principal usada foi o Google Acadêmico, onde foram utilizadas determinadas palavras chaves, a partir da (Tabela 1) é possível visualizar a quantidade de resultados retornados por palavra chave. Os critérios de inclusão usados sobre os artigos foram referentes aos tópicos citados acima.

Tabela 1. Resultados Encontrados

Palavra Chave:	**Resultados Retornados:**
Redes SDN	3.850 resultados.
Redes Definidas por Software	83.500 resultados
Software Defined Networks	4.900.000 resultados
Vantagens redes SDN	419 resultados

Fonte: Dados da pesquisa.

3. Revisão de Literatura

"A utilização de redes SDN vem crescendo não só em aplicações de pesquisa, mas também na indústria" (ANDRIOLI, ROSA RICHI e AUBIN,2017, p. 11). Desta forma podemos perceber que essa tecnologia vem ganhando público tanto acadêmico como de negócios. Seu princípio partiu da iniciativa *open source* (código aberto), que deu base para sua criação, "Com o crescimento de iniciativa *open source*, estamos saindo de um cenário onde o ecossistema de serviços e infraestrutura era fechado e proprietário e passa a ser aberto e livre" (Yap, 2010b, apud AVELAR et al,2013, p. 1).

Existem diferentes trabalhos relacionados a esse novo paradigma, em grande maioria evidenciam o problema. "A comunidade de redes se encontra hoje em uma situação complexa: o sucesso da área pode ser considerado estrondoso, já que hoje a tecnologia de redes de computadores permeia todos os níveis da sociedade", (GUEDES, 2012, P. 1). Em outro estudo, Soares et.al (2019, p.1), diz que

> As redes de telecomunicações tornaram-se uma das principais fontes de informação a nível mundial. Em consequência do sucesso e popularização, surgiram vários problemas para manter a qualidade nos diferentes tipos de tráfego, o que encarece a entrega dos serviços das redes corporativas, tais como: a transmissão de tráfego de voz, dados e streaming de vídeos. (SOARES, et al, 2019, p.1).

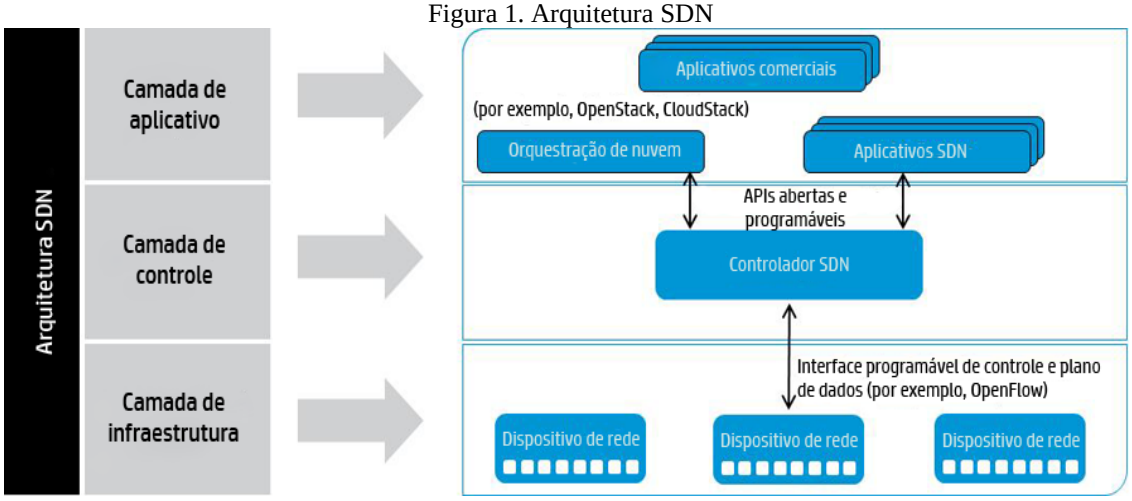
Evidenciando tais problemas citados nas redes tradicionais atuais, fica claro a necessidade da inovação na área. Com o avanço da tecnologia, a atualização e criação de novos

recursos são essenciais para a modernização deste meio. E Menezes (KREUTZ et al, 2015, apud MENEZES et al, 2018, p. 1), quem diz:

> Software Defined Network (SDN) é um novo paradigma para as redes de computadores que muda a maneira de gerenciar, administrar e controlar a rede de computadores, quebrando as limitações impostas das redes atuais ao desacoplar o plano de controle, relacionado ao controle do tráfego de rede, do plano de dados, responsável por encaminhar o tráfego em acordo com o plano de controle (KREUTZ et al, 2015, apud MENEZES et al, 2018, p. 1).

"A disseminação de SDN vem gerando inúmeros trabalhos e pesquisas em torno desse modelo" (MARTINS et al. 2018). Diversos trabalhos vêm sendo publicados a respeito da arquitetura por trás das redes SDNs. É possível perceber a arquitetura SDN por meio da (Figura 1), em que é composta por três camadas principais. A camada de infraestrutura fica responsável pelo plano de dados e encaminhamento de pacotes, formada por switches e roteadores específicos, que juntos formam o conjunto de elementos. A camada de controle e o núcleo da rede e definida por software, formada por um controlador centralizado, possibilitando assim a programação da mesma. Onde esse controlador fornece uma visão global de toda infraestrutura da rede para camada de aplicação. (ANDRIOLI, ROSA RICHI e AUBIN,2017).

Figura 1. Arquitetura SDN



Fonte: SOLUÇÕES INDUSTRIAIS, 2019.

Outros trabalhos exploram como é possível realizar o gerenciamento da rede, e outras características. Leal et al. (2017), demonstra um estudo comparativo com a utilização de equipamentos de redes convencionais, e o uso da SDN simulado em um ambiente virtual, onde busca evidenciar a eficiência e estabilidade proporcionada pela SDN. A tarefa para avaliação foi a mudança do endereço IP do *gateway* da rede, e usou o tempo de parada de reinicialização do *gateway* como métrica da experimentação. Entre os resultados obtidos, os pontos de acesso tradicionais tiveram tempos de paradas distintos, onde o primeiro ficou em média 67 segundos, e o outro, 84 segundos para reinicializar, já no ponto de acesso com a SDN a alteração do *gateway* foi automática, sem tempo de parada para reinicializar, dessa forma deixa a tarefa de alteração de IP independente dos serviços da

rede, dando ao administrador o controle de conexão em tempo real, sem afetar o restante dos serviços.

O artigo apresentado por, Oliveira et al. (2018), propõe uma solução utilizando o ambiente SDN, para gerenciamento de tráfego de dados em infraestruturas de redes hospitalares, partindo do problema em que dispositivos e sistemas médicos dedicados a saúde que são integrados a sistemas de TI, estão conectados à mesma rede de toda arquitetura hospitalar onde ocorre o compartilhamento da rede por outros dispositivos, podendo assim comprometer a qualidade de serviço nos equipamentos que necessitam de uma rápida comunicação. Como solução, e proposto um gerenciamento utilizando recursos da rede SDN, priorizando o tráfego dos dispositivos médicos mais críticos. O monitoramento fica responsável por parte da central que verifica atrasos de recepção ou alarmes enviados dos dispositivos. Um controlador SDN localizado na central de monitoramento fica responsável por gerenciar os *switches* da rede, priorizando os dispositivos críticos em relação aos outros conectados a rede.

Para prover uma melhor justiça em aplicações interativas, Silva, Couto e Rubinstein (2018), propõe uma aplicação utilizando uma rede SDN de longa distância para minimizar as diferenças entre latências de múltiplos usuários conectados em um único servidor. Os usuários conectam-se a um servidor utilizando uma rede SDN, o controlador aplica um cálculo de caminho para cada usuário, assim força que a latência seja igual para todos os usuários que estão conectados ao servidor.

Oliveira et al. (2018), apresenta um estudo sobre a arquitetura de provisão de qualidade de serviço (*Quality of Service* – QoS), explorando as capacidades das redes SDNs, trazendo a problemática da crescente demanda por aplicações distribuídas de alto desempenho, e as limitações e dificuldades administrativas e econômicas atribuídas às redes tradicionais para tal demanda. O modelo proposto disponibiliza um protótipo desenvolvido dos componentes da arquitetura de QoS, a partir de reserva de recursos e priorização de tráfego de dados , onde o administrador da rede disponibiliza classes de serviços a partir de uma estrutura de dados, onde são acessadas por elementos do ambiente, desta forma componentes são chamados pelas aplicações distribuídas por meio de funções e estabelecem requisitos específicos de QoS entre comunicação e controlador SDN, onde todo a processo e monitorado pelo controlador SDN, que insere filas de QoS aos fluxos particulares de pacotes dos componentes de encaminhamento, ao longo de todo tráfego entre provedor e cliente. Para monitoramento dos resultados, foi desenvolvido um ambiente virtual SDN, que a partir de simulações definidas com transferência de arquivos com tamanhos diferentes, foram avaliados os tempos de sobrecarga em cada teste. Nas avaliações dos resultados foi possível perceber a eficácia da arquitetura, que apresentou baixa sobrecarga em todo tempo de transferência e redução significativamente de tempo de transmissão.

Em questões voltadas a segurança, Campos e Martins (2017), demonstram em seu estudo a exploração de recursos da rede SDN a partir de uma arquitetura de segurança de rede, com objetivo de implementar mecanismos para detecção e reação em ameaças de segurança, tratando diferentes tipos de vulnerabilidades nas redes SDN e explorando como os novos recursos dessa tecnologia podem ajudar na prevenção e investigação voltados para a segurança. Onde a partir da realização de testes maliciosos, a rede se mostrou inovadora, com auxílio de sistemas de detecção juntamente com recursos de controle da rede, foi possível detectar potenciais ataques, como também controlar

possíveis perigos, além da inclusão de ameaças a lista negra e exibição para o administrador, como reação.

Com a utilização de uma rede SDN, Pinheiro, Burgardt e Campelo (2018), apresentam uma solução de pseudo-anonimização na utilização de dispositivos de internet das coisas (*Internet of Things*, IoT). Como os dispositivos de IoT obtém dados de seus usuários, são alvos de possíveis ataques maliciosos utilizando endereços IP e MAC de seus dispositivos. Como solução, configuram os *switches* SDN para ocultar endereços e portas e substituí-los por pseudônimos que são criados de forma aleatória pelo controlador, obtendo maior privacidade no uso de dispositivos IoT.

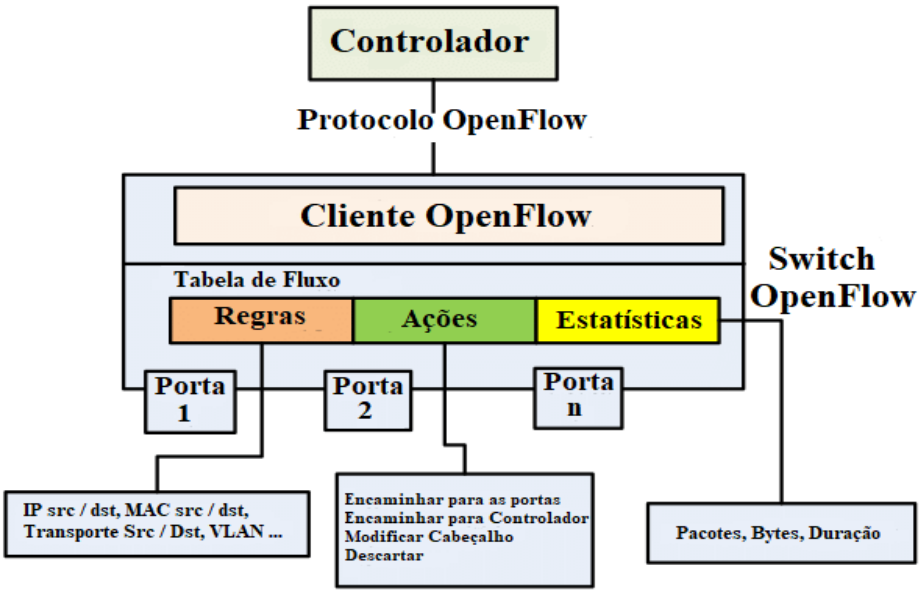
Oliveira (2019), propõe uma rede SDN para prover uma comunicação de dados mais eficiente em ambientes de *Big Data* e HPC (Computação de alto desempenho), visto que estas aplicações necessitam de uma infraestrutura com alto poder computacional. Pelo fato das redes SDN possuírem um maior nível de programabilidade, por meio de uma API o controlador e informado sobre aplicações paralelas e distribuídas que está recebendo, assim gerencia de forma adequada o roteamento de cada perfil de tráfego, de acordo com as configurações estabelecidas pelo administrado, tornando a rede mais eficiente e flexível para atender as aplicações. Os resultados obtidos mostraram que o uso da arquitetura SDN no problema exposto, mostrou-se ser eficaz reduzindo tempos de execução de ambas aplicações.

Entretanto um dos pontos mais citados e sobre o funcionamento do protocolo OpenFlow. Segundo Rodrigues et al (2015):

> O OpenFlow é um dos principais protocolos relacionados a SDN e, de fato, é o que possibilita a implementação desse novo paradigma. Com a padronização do OpenFlow, vendedores e operadores de rede começam a dar uma importância maior a ele, reforçando por consequência o paradigma SDN (RODRIGUES et al, 2015, p.3).

A arquitetura OpenFlow reproduzida por Nunes et.al (2014), (Figura 2), uniformiza a troca de informações entre dois planos, o comutador com as tabelas de fluxo e a camada de abstração que se comunica com o controlador. Onde as entradas de fluxos são compostas por campos de correspondência com o cabeçalho do pacote, os contadores para o controle de fluxo, e o conjunto de instruções com as regras a serem aplicadas.

Figura 2. Arquitetura OpenFlow



Fonte: Adaptado de NUNES et.al, 2014, p. 4.

Apesar de existirem outras tecnologias, o protocolo OpenFlow segue com uma principal aposta, devido a criação de uma organização para o seu desenvolvimento pelas indústrias. (ONF, 2013, apud, FERNANDES; ROTHENBERG, 2014).

> A vantagem do protocolo OpenFlow é que com sua utilização, pesquisadores podem testar suas experiências sem que interfira no tráfego real da rede de produção e sem a necessidade que os fabricantes de comutadores exponham os projetos de software e hardware dos seus equipamentos (COSTA, 2013, p.21).

Oliveira et al. (2017), apresenta um trabalho em ambiente de experimentação OpenFlow, onde analisa e verifica pontos fortes e fracos de acordo com a ferramenta utilizada, com intuito de auxiliar pesquisadores da área, a partir do desempenho alcançado em cada ambiente de experimentação. Onde por meio de topologias emuladas e ambientes físicos igualmente limitados, avaliou impactos de processamento dos dispositivos, impactos no plano de controle de acordo com a plataforma adotada, tempo de processamento entre a chegada e geração de eventos pelo controlador, tempo de requisições e análise de conexões com foco em atraso de pacotes.

Para prover melhor orquestração em uma rede SDN, Soares e Lucena (2018), descrevem em seu artigo o serviço Havox, que auxilia o administrador na programação do comportamento da rede, de forma simplificada e de alto nível. O serviço Havox gera múltiplas regras OpenFlow, a partir da plataforma de roteamento IP RouteFlow, e do gerenciador de regras de fluxo o *framework* Merlin. Os testes apontaram que a partir de uma única diretiva de serviço, foram geradas regras OpenFlow de acordo com o crescimento da rede, permitindo ao administrador que apenas configure políticas de orquestração, sem a necessidade de inserção de novas regras OpenFlow.

Entre os controladores baseados no protocolo OpenFlow, o NOX foi o projeto inicial baseado na linguagem C/C++, os mesmos criadores desenvolveram logo após o controlador POX baseado na linguagem Python, que em comparação resulta que o POX tem melhor latência que o NOX (FERREIRA, 2016). Outro que se destaca é o “Beacon é um controlador OpenFlow modular, multiplataforma e que suporta tanto operações

baseadas em eventos quanto processos multi-thread (ERICKSON, 2013, apud, RODRIGUES, GUIMARAES, 2014, p. 43)".

Outras ferramentas que podem trabalhar juntamente com o OpenFlow são os simuladores de redes SDNs, "A ferramenta Mininet pode criar elementos SDN, customizá-los, compartilhá-los com outras redes e realizar interações. Esses elementos incluem hosts, switches, roteadores e links (conexões). (OLIVEIRA et al, 2014, apud, BOGO JUNIOR, 2017, p. 26)".

Costa et al. (2018), propõe uma ferramenta de administração de perfis de usuários para permissão de acesso aos recursos da rede, a partir dos fluxos dos dispositivos. A ferramenta utiliza o controlador POX, onde coleta informações dos dispositivos conectados e verifica em um banco de dados se está associado a algum perfil de usuário, autorizando o acesso aos perfis de usuários com privilégios e acesso padrão aos usuários sem privilégios. Os resultados obtidos tiveram total sucesso na administração de diferentes perfis de usuários conectados rede.

Na virtualização em *data centers*, Souza et al. (2017), aborda uma infraestrutura baseada em SDN denominada QVIA-SDN (*Quality-Aware Virtual Infrastructure Allocation SDN*), que aloca o modelo IV (Infraestruturas Virtuais) em data center na nuvem com switches OpenFlow. Os testes foram realizados comparando o lado provedor do *data center*, a latência no lado cliente e a configuração da IV. Os resultados obtidos após a realização de testes mostram uma redução na latência, além de respeitar o QoS imposta pelo provedor.

Em experimentações envolvendo a rede SDN, Lima et al. (2018), elabora uma arquitetura de rede baseada em SDN, utilizando o controlador Floodlight, que também já possui o protocolo OpenFlow, no ambiente simulado utilizando a ferramenta Mininet. O objetivo é comparar os resultados entre a utilização do controlador nativo da ferramenta, e o controlador Floodlight, onde para realização dos testes foram feitas alterações no simulador Mininet, para que o mesmo utilizasse o controle externo. A partir de testes realizados, como resultados foi possível observar que em vários casos o controlador externo Floodlight obteve resultados iguais ou melhores sobre o controlador utilizado pela ferramenta Mininet.

Vieira Jr et al. (2017), apresenta uma solução utilizando a rede SDN para redução de recursos em servidores VoIP (*Voice over Internet Protocol*). O serviço VoIP compartilha recursos da mesma rede de outros dispositivos, onde um grande número de chamadas simultâneas aumenta o consumo de CPU e largura de banda do servidor. Como solução, s*witches* SDN são instalados na rede onde ocorre o tráfego de comunicação VoIP e são configurados com uma tupla de informações para reconhecerem o tráfego VoIP, ao reconhecer chamadas com mesmo *Codec* (codificador/decodificador), os switches SDN conectam as chamadas diretamente, sem a necessidade da comunicação trafegar pelo servidor VoIP, desta forma economizando recursos de largura de banda e consumo de CPU.

Sobre as desvantagens nas redes SDN, existem estudos que buscam apresentar pontos que precisam ser melhorados, em grande parte são voltados a segurança e arquitetura da rede. Pascoal (2018), destaca que as redes SDN por apresentarem em sua arquitetura o controle centralizado, fica mais vulnerável a possíveis ataques, desta forma ao interromper a atividade do controlar toda rede para de funcionar. Outro ponto abordado são ataques

relacionados a negação de serviço, pelo fato dos *switches* SDN possuírem armazenamento limitado, assim como nas redes tradicionais, fica vulnerável a ataques de saturação e exaustão a tabela TCAM (*Ternary Content-Addressable Memory*), onde força a instalação de novas regras pelo controlador na tabela de fluxo do *switch* SDN. No ataque de saturação ocorre o aumento da comunicação entre o controlador e o *switch*, causando um *overhead* na rede, já no ataque de exaustão acontece o estouro de memória de armazenamento, assim novas regras não são instaladas. Um outro ataque semelhante identificado e o Slow TCAM, onde ocorre a exaustão da tabela TCAM do *switch* sem a necessidade de grande tráfego na rede, o atacante utiliza uma *botnet* onde cada *bot* envia um pacote para o *switch*, para cada pacote e instalada duas novas regras de fluxo, uma regra de chegada e uma de saída da rede, o atacante coordena a criação dos pacotes e faz a configuração para que cada *bot* envie seus pacotes de forma lentamente, a fim de evitar o detecção do ataque pelo administrador da rede. Como defesa e proposto o SIFT (*Selectlve Defense for TCAM*), que utiliza o controlador da rede e funções do protocolo OpenFlow. Quando a tabela TCAM do *switch* está cheia, o SIFT é acionado e decide usando uma probabilidade se a regra será instalada ou não.

Centeno (2016), indica em seu estudo, algumas vulnerabilidades nas redes SDN sobre o protocolo OpenFlow, como falta de autenticação de origem, canal de comunicação inseguro, vulnerabilidades de componentes, negação de serviço, e expõe que apesar das vantagens em tecnologia e administração, falhas de segurança voltadas ao protocolo OpenFlow, afetam as redes SDN, seja no plano de dados ou de controle. A partir da (tabela 2), é possível perceber as vulnerabilidades citadas, e os planos que estão expostos a possíveis ataques.

Tabela 2 – Vulnerabilidades / plano exposto

Vulnerabilidade	**Plano de Controle**	**Plano de dados**
Falta de autenticação de origem	Sim	Sim
Canal de comunicação inseguro	Sim	
Vulnerabilidade de componentes	Sim	
Negação de Serviço	Sim	Sim

Fonte: Adaptado de CENTENO, 2016, p.31

4. Resultados e análise dos resultados

Artigos foram explorados com o intuito de representar vantagens obtidas no emprego das redes definidas por software é outras características de sua arquitetura. Entre as principais vantagens constatadas, é possível perceber a partir da (Tabela 3), a descrição de alguns benefícios mais influentes na adoção da arquitetura SDN.

Tabela 3 - Vantagens Arquitetura SDN

Descrição:	Características:
Diretamente programável:	O controle de rede é diretamente programável porque é desacoplado das funções de encaminhamento.

Gerido Centralmente	A inteligência de rede é centralizada (logicamente) em controladores SDN baseados em software que mantêm uma visão global da rede, que aparece para aplicativos e mecanismos de políticas como um único switch lógico.
Configurado Programaticamente	O SDN permite que os gerentes de rede configurem, gerenciam, protejam e otimizem os recursos de rede muito rapidamente por meio de programas SDN dinâmicos e automatizados, que eles mesmos podem escrever porque os programas não dependem de software proprietário.
Aberto a Padrões	Quando implementada por meio de padrões abertos, a SDN simplifica o projeto e a operação da rede porque as instruções são fornecidas pelos controladores SDN, em vez de vários dispositivos e protocolos específicos do fornecedor.

Fonte: Adaptado de OPEN NETWORKING FOUNDATION, 2019.

A partir das características descritas, fica notório a simplicidade e robustez na administração de uma rede SDN, o ganho de recursos de gerenciamento a partir da programação dos planos de dados e controle, possibilita a adaptação dos serviços de toda a rede de acordo com complexidade e infraestrutura.

Na aplicação de pesquisas e experimentação, com auxílio da tecnologia de virtualização de máquinas, estudantes e pesquisadores podem realizar testes de forma prática e segura, na tentativa de obter novos recursos como o de controle da rede, provisão de qualidade de serviços, monitoramento de atividades e recursos, balanceamento de carga de fluxo dados, e outras possibilidades a serem exploradas. Entretanto ainda é necessário a busca de novos recursos, a fim de alcançar melhores resultados e obter melhor segurança.

5. Conclusão

A partir do estudo apresentado, é possível perceber a importância das redes de computadores para prover melhor conectividade entre infraestruturas e principalmente obter melhor comunicação de fluxo de dados na internet global, para comportar as diferentes tecnologias que utilizam arquiteturas de rede e internet.

Entre outras características as redes SDN vem ganhando espaço na infraestrutura atual. As principais vantagens identificadas mostram que a rede SDN proporciona um novo e melhor modelo de gerenciamento e administração da rede, auxilia estudantes e pesquisadores em busca de novo recursos, provisiona uma melhor qualidade de serviço (QoS) em aplicações críticas e interativas, proporciona um alto nível de programação da rede. Entretanto, pelo fato de possuir um plano de controle totalmente centralizado, as redes SDN ficam vulneráveis a possíveis ataques maliciosos ao plano de controle, também foram identificados ataques de negação de serviço nos dois planos dados/controle que prejudica desempenho da rede.

Com a finalidade de mitigar problemas e suprir obstáculos nas redes tradicionais. As redes definidas por softwares revelam-se como uma arquitetura inovadora, onde a partir de plataformas *open source*, conseguem obter ferramentas essenciais e importantes, ao ser implementada com outras tecnologias para contornar os principais problemas atuais da área.

Como trabalhos futuros, pretende se desenvolver novos recursos utilizando o ambiente SDN, voltados a administração de serviços de rede, detecção de falhas em infraestruturas, prevenção a possíveis ataques.

6. Referências

ANDRIOLI, Leandro; DA ROSA RIGHI, Rodrigo; AUBIN, Mateus Rauback. Analisando métodos e oportunidades em redes definidas por software (SDN) para otimizações de tráfego de dados. Revista Brasileira de Computação Aplicada, 2017, 9.4: 2-14.

AVELAR, Edson Adriano Maravalho; AVELAR, Lorena Marques; DIAS, Kelvin Lopes. Pmipflow: Uma proposta para gerenciamento de mobilidade em redes definidas por software. 2013. PhD Thesis. Master's thesis, Universidade Federal de Pernambuco.

BOGO JUNIOR, José. Uso da ferramenta mininet para estudo de redes definidas por software. 2017. Bachelor's Thesis. Universidade Tecnológica Federal do Paraná.

CENTENO, Paulo Vieira. Uma análise de segurança de Redes Definidas por Software sobre protocolo OpenFlow**.**2016. 83 f. TCC (Graduação) - Curso de Sistemas de Informação, Centro Tecnológico da Ufsc, Universidade Federal de Santa Catarina, Florianópolis, 2016.

COMER, Douglas E. Redes de Computadores e Internet-6. Bookman Editora, 2016.

CAMPOS, Maxli Barroso; MARTINS, Joberto. Uma proposta de arquitetura de segurança para a detecção e reação a ameaças em redes SDN. Revista Brasileira de Computação Aplicada, 2017, 9.1: 107-119.

COSTA, Christiano M., et al. Aplicação de SDN no gerenciamento de perfis de usuário em dispositivos de rede. In: Anais do Workshop de Trabalhos de Iniciação Científica e Graduação (WTG-SBRC 2018). SBC, 2018.

COSTA, Lucas Rodrigues. OpenFlow e o paradigma de redes definidas por software. 2013.

FERNANDES, Eder Leao; ROTHENBERG, Christian Esteve. OpenFlow 1.3 software switch. Salao de Ferramentas do XXXII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuıdos SBRC, 2014, 1021-1028.

FERREIRA, Caio César, et al. Análise comparativa de controladores para redes definidas por software de Classe Carrier Grade. 2016.

FOROUZAN, Behrouz A. Comunicação de dados e redes de computadores. AMGH Editora, 2009.

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: 160-210.

INTERNET WORLD STATS. Internet Usage Statistics. 2019. Disponível em: <https://www.internetworldstats.com/stats.htm>. Acesso em: 27 maio 2019.

LEAL, Rodrigo et al. Um Comparativo entre as Redes Definidas por Software e Redes Tradicionais. 2017. 6 f. TCC (Graduação) - Curso de Computação, Departamento de Computação, Universidade Federal do Piauí (ufpi), Picos – Pi – Brasil, 2017.

LIMA, João Carlos, et al. Análise da aplicação do Floodlight em um ambiente SDN. In: Anais da IV Escola Regional de Informática do Piauí. SBC, 2018. p. 208-213.

MARTINS, Bruno José Cesário de Almeida, et al. Provisão de Qualidade de Serviço em Redes Definidas por Software. Relatórios Técnicos do DCC/UFJF, 2018.

MENEZES, Pablo Marques, et al. Estudo Catalográfico sobre Redes Definidas por Software (SDN) no âmbito brasileiro. Semana de Pesquisa da Universidade Tiradentes-SEMPESq, 2018, 18.

NUNES, Bruno Astuto A., et al. A survey of software-defined networking: Past, present, and future of programmable networks. IEEE Communications Surveys & Tutorials, 2014, 16.3: 1617-1634.

OLIVEIRA, Alexandre T., et al. Arquitetura de Provisão de Qualidade de Serviço para Aplicações Distribuídas de Alto Desempenho em Redes Definidas por Software. In: Anais do XXIII Workshop de Gerência e Operação de Redes e Serviços (WGRS-SBRC 2018). SBC, 2018.

OLIVEIRA, Alexandre Tavares de. Uma plataforma de rede definida por software para ambientes de computação paralela e distribuída. 2019. 65 f. Dissertação (Mestrado) - Curso de Programa de Pós-graduação em Ciência da Computação, Ice – Instituto de Ciências Exatas, Universidade Federal de Juiz de Fora (ufjf), Juiz de Fora, 2019.

OLIVEIRA, Lucas B., et al. Uma Abordagem SDN para Priorização de Tráfego em Ambientes Hospitalares Inteligentes. In: 18º Simpósio Brasileiro de Computação Aplicada à Saúde (SBCAS 2018). SBC, 2018.

OLIVEIRA, Rodrigo A. de et al. Analisando o Comportamento de Ambientes de Experimentação baseados em OpenFlow. In: Anais do XXII Workshop de Gerência e Operação de Redes e Serviços (WGRS-SBRC 2017). SBC, 2017.

OPEN NETWORKING FOUNDATION. Software-Defined Networking (SDN) Definition. 2019. Disponível em: <https://www.opennetworking.org/sdn-definition/>. Acesso em: 17 maio 2019.

PASCOAL, Túlio Albuquerque. Atacando e Defendendo Redes Definidas por Softwares. 2018. 98 f. Dissertação (Mestrado) - Curso de Pós-graduação em Informática, Centro de Informática, Universidade Federal da Paraíba, João Pessoa - Pb, 2018.

PINHEIRO, Antonio J.; BURGARDT, Caio AP; CAMPELO, Divanilson R. Preservando a Privacidade na Internet das Coisas com Pseudônimos Usando SDN. In: SBSeg 2018. SBC, 2018. p. 121-128.

RODRIGUES, Cristiane P., et al. Avaliação de Balanceamento de Carga Web em Redes Definidas por Software. 2015.

RODRIGUES, Thiago Nascimento; GUIMARÃES, Rafael Paoliello. Usabilidade de controladores OpenFlow: uma proposta de avaliação baseada em arquiteturas de código-fonte. Abakós, 2014, 3.1: 38-58.

SILVA, Felipe AF da; COUTO, Rodrigo S.; RUBINSTEIN, Marcelo G. Utilizando Redes Definidas por Software para Prover Justiça em Aplicações Interativas. In: Anais do XXXVI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. SBC, 2018.

SOARES, André G. Lima et al. ESTUDO DA IMPLEMENTAÇÃO DE VoIP EM REDES SDN. Disponível em: <http://www.unibratec.edu.br/tecnologus/wp-content/uploads/2015/12/tecnologus_edicao_09_artigo_06.pdf>. Acesso em: 17 maio 2019.

SOARES, Rodrigo, et al. Havox: Um serviço para orquestração de tráfego em alto nível em redes OpenFlow. In: Anais do XXIII Workshop de Gerência e Operação de Redes e Serviços (WGRS-SBRC 2018). SBC, 2018.

SOLUÇÕES INDUSTRIAIS (Ed.). SOFTWARES DE CONTROLES DE REDES E DE CRIAÇÃO DE IMAGENS. Disponível em: <https://www.solucoesindustriais.com.br/empresa/identificacao_etiquetagem_e_radio_frequencia/markem-imaje-identificacao-de-produtos-ltda/produtos/software/software-de-controle-de-rede-e-de-criacao-de-imagem>. Acesso em: 16 maio 2019.

SOUZA, Felipe Rodrigo de, et al. Alocação de Infraestruturas Virtuais em data centers implementados com Redes Definidas por Software. In: Anais do XXXV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. SBC, 2017.

TANENBAUM, Andrew S. Redes de computadores Quarta edição. Editora Campus, 2003.

VIEIRA JR, Paulo Roberto, et al. Gerenciamento de recursos de serviços de Voz sobre IP baseado em Redes Definidas por Software. In: Anais do XXII Workshop de Gerência e Operação de Redes e Serviços (WGRS-SBRC 2017). SBC, 2017.