Uma Taxonomia para Descrever e Caracterizar Estratégias de Mitigação de Ataques DDoS em Ambientes IoT Usando Tecnologias SDN

Esau Silva[1], Felipe S. Dantas Silva [1,2], Marcilio O. O. Lemos[1,2], Augusto Venâncio Neto [2,3]

[1]LaTARC Research Lab
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (IFRN)
Natal-RN, Brasil

[2]Departamento de Informática e Matemática Aplicada (DIMAp)
Universidade Federal do Rio Grande do Norte (UFRN) – Natal-RN, Brasil

[3]Instituto de Telecomunicações (IT), Aveiro, Portugal

esau.silva@academico.ifrn.edu.br, felipe.dantas@ifrn.edu.br
marcilio.cc.lemos@gmail.com, augusto@dimap.ufrn.br

Abstract. *The Internet of Things has attracted significant attention from the Information and Communication Technology (ICT) community through the perspective of everyday objects collecting data from the environment and transmitting them via the Internet for post-processing, without the need for human-computer interaction . Although IoT represents a powerful platform for creating new products and services that will benefit a wide variety of verticals industries (e-health, V2X, smart homes, etc.), there are a number of security concerns that need be remedied for their proper implementation, such as vulnerabilities exploited by malicious agents to take control of devices and deliver DDoS attacks on a large scale. Therefore, research was initiated to develop solutions for the detection and containment of IoT-based DDoS attacks, making use of emerging technologies such as the Software Defined Networks (SDN) paradigm. In this sense, the present work presents a taxonomy to describe and characterize the body of SDN solutions against DDoS attacks in IoT scenarios.*

Resumo. *A Internet das Coisas têm atraído significativa atenção da comunidade de Tecnologia da Informação e Comunicação (TIC) pela perspectiva de objetos do cotidiano coletando dados do ambiente e transmitindo-os através da Internet para processamento a posteriori, sem que haja necessidade de interação humano-computador. Embora a IoT represente uma poderosa plataforma para criação de novos produtos e serviços que irão beneficiar uma ampla variedade de verticais (e-health, V2X, smart homes, etc), existem diversas preocupações de segurança que precisam ser remediadas para sua implementação adequada, como as vulnerabilidades explorados por agentes maliciosos para assumir o controle de dispositivos e desferir ataques DDoS em larga escala. Por conseguinte, pesquisas foram iniciadas para desenvolver soluções visando a detecção e contenção de ataques DDoS baseados em IoT, fazendo uso de tecnologias emergentes como o paradigma de Redes Definidas*

por Software (SDN). Neste sentido, o presente trabalho apresenta uma taxonomia para descrever e caracterizar o corpo de soluções SDN contra ataques DDoS em cenários da IoT.

1. Introdução

A Internet das Coisas (IoT, do inglês *Internet of Things*) [Al-Fuqaha et al. 2015] promete revolucionar a ideia que as pessoas têm dos computadores em seu dia a dia, transformando dispositivos em elementos onipresentes que realizam computação de maneira transparente para seus usuários. Por meio do paradigma IoT, a entrega de serviços fornecerá níveis de comodidade sem precedentes, mas que também adicionam novas preocupações de segurança que podem ofuscar seus benefícios [Noor and Hassan 2019].

Na maioria dos cenários IoT, dispositivos interagem com aplicações que são executadas remotamente na rede, o que possibilita a ação de agentes maliciosos que podem assumir o controle dos dispositivos. Desta maneira, é possível haver a interrupção de serviços ou a utilização de dispositivos como ponto de lançamento de ataques para domínios diversos. De fato, o aumento explosivo no tamanho dos Ataques de Negação de Serviço Distribuído (DDoS, do inglês *Distributed Denial of Service*) [Zargar et al. 2013] observados nos últimos anos é frequentemente associado a popularização de aplicações impulsionadas pela IoT. Muitos desses ataques foram bem-sucedidos em interromper serviços básicos da Internet, como o DNS, afetando milhões de usuários ao redor do mundo [Marzano et al. 2018], e gerando severas perdas financeiras as organizações que mantêm esses serviços.

Naturalmente, este cenário criou uma nova demanda por tecnologias que forneçam maneiras mais eficientes de proteger a integridade de serviços de rede frente a ataques DDoS originados por dispositivos IoT. Neste contexto, a relativa facilidade na execução de ataques DDoS em larga escala aumenta a preocupação com segurança ao passo da proliferação das atividades das redes zumbis (*botnets*) [Bertino and Islam 2017]. Um exemplo dentro deste contexto é a *botnet* Mirai [Kolias et al. 2017] [Marzano et al. 2018], que em 2016 indisponibilizou grande parte do acesso à Internet em diversos países. Frente a isso, operadores de rede e pesquisadores dedicaram diversos esforços para endossar níveis adequados de segurança em infraestruturas IoT para impedir que atividades deste tipo sejam realizadas.

Nesse contexto, o advento de tecnologias como as Redes Definidas por Software (SDN, do inglês *Software-Defined Networking*) [Koufopavlou 2015] é considerada pela comunidade de pesquisa como um dos principais avanços tecnológicos na área de redes pela perspectiva de flexibilidade e programabilidade das infraestruturas. A tecnologia SDN envolve o uso de substratos definidos por software, que desacoplam o plano de controle do plano de dados, permitindo assim que funções antes executadas em hardware, pelos nós da infraestrutura de rede, agora passem a ser executadas ao nível de software hospedado em controladores centralizados. Além disso, APIs comuns implementadas tanto pelos controladores SDN quanto pelos nós de rede fornecem a capacidade de (re)programação do sistema em tempo de execução. Nessa abordagem centralizada, controladores SDN podem supervisionar e atuar na infraestrutura, tendo como apoio bases de conhecimento acerca de todo sistema adjacente. Assim, é possível ter acesso, por meio de uma visão holística, a todo a infraestrutura da rede, incluindo os serviços e aplicações,

maximizando as perspectivas de detecção e contenção de ameaças.

Inúmeros estudos adotaram SDN como meio de implementar níveis de segurança nas infraestruturas de rede em diversos segmentos, tais como controle de acesso [Yakasai and Guy 2015], detecção de malwares [Ceron et al. 2016], comunicação confiável de dados [Shi et al. 2017], dentre outros. Recentemente, várias propostas também fizeram uso da abordagem SDN para fornecer proteção às infraestruturas diante das iminentes ameaças causadas por ataques DDoS [Kalkan et al. 2017]. Com esta motivação novas soluções foram empregadas com o intuito de avançar as atuais estratégias para modelos com capacidades avançadas que fornecessem aos operadores de rede a flexibilidade necessária para aprimorar suas defesas diante da evolução dos ataques.

Mesmo SDN tendo sido amplamente empregada no desenvolvimento de novos algoritmos, soluções e estratégias de detecção e contenção de DDoS para serem aplicados de forma eficiente na proteção das infraestruturas, poucos estudos se comprometeram em fornecer uma visão abrangente de sua aplicação no cenário IoT. Isso se faz necessário à medida em que existe uma grande evolução na variação e ação dos atacantes, bem como nos efeitos causados pelas ameaças, de modo que os desenvolvedores possam guiar-se durante a concepção de novas ferramentas. Em levantamento recente do estado da arte, pode-se identificar que poucos trabalhos se comprometeram a fornecer uma visão abrangente das principais soluções propostas para mitigação de ataques DDoS em ambientes IoT através do uso da tecnologia SDN. Esta lacuna é a principal motivação deste estudo uma vez que se faz necessário identificar as principais abordagens propostas neste meio, de modo que se possa compreender claramente suas vantagens e desvantagens e reconhecer as ações esperadas por mecanismos de defesa diante de determinadas situações de ameças impostas pela variabilidade dos ambientes IoT. Em função disso, este trabalho introduz uma taxonomia para descrever e caracterizar as estratégias de mitigação de ataques DDoS que fazem uso da tecnologia SDN, em ambientes IoT.

As principais contribuições fornecidas neste trabalho podem ser sumarizadas da seguinte maneira: sólida classificação das estratégias de mitigação DDoS usando SDN sob diferentes perspectivas, tais como o local de implantação, limitações, estratégia de detecção e mitigação adotada, bem como abrangência na quantidade de soluções revisadas e escopo (diferente dos trabalhos relacionados que concentram-se apenas nos aspectos de segurança em ambientes IoT).

O restante deste trabalho está organizado da seguinte maneira: a Seção 2 aponta os trabalhos relacionados ao tema de pesquisa descrito; a Seção 3 detalha a metodologia adotada na condução desta taxonomia; a Seção 4 apresenta a taxonomia das soluções estudadas; a Seção 5 apresenta a classificação das estratégias revisadas;Por fim na Seção 6 são apresentada as considerações finais e os direcionamentos para trabalhos futuros.

2. Trabalhos Relacionados

Atualmente existem na literatura diversos trabalhos com a proposta de revisar soluções de segurança para diversos problemas em ambientes IoT, como confidencialidade, integridade, controle de acesso, disponibilidade etc. Neste sentido [Kouicem et al. 2018] desenvolveu um estudo sobre os principais desafios de segurança inerentes a importantes áreas de aplicação IoT, como *e-health*, *smart grids*, *smart cities*, dentre outros. Além disso os autores levantaram e classificaram diversas soluções de segurança nesse contexto,

levando em consideração principalmente *(i)* se a solução é baseada em tecnologias emergentes (ex. SDN e *blockchain*) ou tradicionais e; *(ii)* segmento do problema de segurança que a solução aborda.

Já o trabalho desenvolvido em [Kanagavelu and Aung 2019] avalia inicialmente a aplicabilidade do paradigma SDN no desenvolvimento de soluções de segurança para IoT. Além disso os autores revisam diversas estratégias de segurança nesse contexto com base em três categorias principais: *(*i) arquiteturas IoT baseadas em SDN; *ii* arquiteturas IoT baseadas em virtualização e SDN; *iii* mitigação de ataques DDoS em IoT baseado em SDN. Neste sentido [Cherian and Chatterjee 2019], [Kalkan and Zeadally 2018] e [Farris et al. 2019] seguiram a tendência dos trabalhos citados anteriormente, classificando os principais problemas de segurança tomando por referência as camadas da infraestrutura IoT e discutindo diferentes soluções que exploram paradigmas emergentes como virtualização de funções de rede (NFV, do inglês *Network Function Virtualization*), aprendizado de máquina (*machine learning*), blockchain e SDN.

Em [Kalkan and Zeadally 2018] os autores apresentaram uma classificação das soluções com base nas seguintes categorias: *(i)* soluções baseadas em rede; *(ii)* soluções baseadas em tráfego e; *(iii)* soluções baseadas em criptografia, analisando suas vantagens e desvantagens. Em contraste, [Farris et al. 2019] concentrou-se em analisar detalhadamente mecanismos de defesa baseados nas tecnologias SDN e NFV.

Seguindo uma perspectiva diferente dos trabalhos citados anteriormente, [Lohachab and Karambir 2018] se empenhou em criar uma taxonomia dos principais tipos de ataques DDoS e suas variações, avaliando o impacto desses ataques em ambientes IoT e revisando diversos mecanismos de defesa, destacando suas principais vantagens e desvantagens. A Tabela 1 sumariza os trabalhos relacionados aqui apresentados, diferenciando-os pelo escopo, quantidade de soluções de mitigação revisadas e sob o aspecto da classificação da mitigação.

Trabalho	**Escopo**	**Quantidade de soluções de mitigação SDN revisadas**	**Classifica as soluções de mitigação?**
[Kouicem et al. 2018]	Segurança em IoT	2	✗
[Kalkan and Zeadally 2018]	Segurança em IoT	1	✗
[Lohachab and Karambir 2018]	Segurança em IoT	1	✗
[Kanagavelu and Aung 2019]	Segurança em IoT	2	✗
[Cherian and Chatterjee 2019]	Segurança em IoT	4	✗
[Farris et al. 2019]	Segurança em IoT	4	✗
Proposta Atual	**Ataques DDoS em IoT**	**9**	✓

Tabela 1. Comparativo entre os trabalhos relacionados

Apesar das contribuições oferecidas pelos trabalhos de revisão citados anteriormente, em apresentar diversas soluções de mitigação, nenhum deles propõe uma revisão sólida, quando se trata de mecanismos de mitigação de ataques DDoS usando o paradigma SDN em redes IoT, capaz de classificar apropriadamente as soluções existentes. Isso se da principalmente pelo fato dos estudos encontrados se limitarem a abordar com pouca profundidade o assunto em questão. Por essa razão este trabalho tem como proposta definir uma taxonomia compreensível das soluções de mitigação no contexto IoT fazendo uso de tecnologias SDN, com a finalidade de fornecer insumos a pesquisadores interessados

no desenvolvimento de novos mecanismos de mitigação.

3. Taxonomia das soluções de mitigação de ataques DDoS

Para conceber uma taxonomia compreensível, neste estudo foram observadas algumas das principais características das soluções de mitigação de ataques DDoS levantadas. Adicionalmente também foram considerados critérios presentes em estudos anteriores de grande relevância. Em função disso, esta seção tem por objetivo justamente discutir detalhadamente esses critérios, como também demonstrar a metodologia de busca utilizada para ampliar a compreensão do leitor.

3.1. Metodologia de busca

Para conduzir o processo de busca foram definidas as seguintes bases de dados de alto impacto em ciência da computação: *(i)* ACM Digital Library; *(ii)* IEEE Xplore; *(iii)* Ingenta Connect; *(iv)* Science Direct; *(v)*Springer Link e; *(vi)* Wiley. Ao final do processo de busca foram obtidos 35 trabalhos. Após a filtragem por título e relevância restaram 9 soluções que foram apropriadamente incluídas e revisadas neste estudo.

3.2. Critérios de classificação

A partir da revisão das soluções de defesa encontradas, foram identificadas três características fundamentais para prover uma categorização consistente das respectivas soluções, são elas: *(i)* Estratégia de detecção; *(ii)* Estratégia de mitigação e; *(iii)* Local de implantação da solução. Estes critérios foram considerados nos estudos anteriores: [Dayal et al. 2016], [Yan et al. 2016] e [Lohachab and Karambir 2018]. Todavia cada autor os considerou de forma individual, enquanto que o presente estudo classifica as soluções de mitigação aqui encontradas na perspectiva dos três critérios em conjunto, fornecendo uma classificação mais ampla e detalhada. Além disso, foram descritas as desvantagens encontradas em cada mecanismo de defesa, conforme é possível observar na tabela 2.

3.2.1. Local de Implantação da solução

As soluções de defesa contra ataques DDoS, podem ser classificadas com base em diversos aspectos, entre eles estão a localização da rede onde são implementadas, como é descrito em [Yan et al. 2016]. Neste sentido, foi observado que os autores optaram por realizar a implantação de duas formas distintas:

- **Na borda da rede:** Pertencem a essa categoria mecanismos locais implementados em um único componente na borda da rede com a finalidade de monitorar tanto o tráfego proveniente quanto o que chega na rede.
- **Distribuída:** Esta categoria engloba as abordagens, implementadas em vários componentes distribuídos em domínios de rede diferentes.

3.2.2. Estratégias de detecção

Outra característica levada em consideração na classificação das soluções é a estratégia utilizada durante o processo de detecção de ataques DDoS, que podem ser divididos da seguinte forma, segundo [Dayal et al. 2016]:

- **Análise estatística:** O objetivo desta técnica é analisar características do tráfego que chega ao sistema e desenvolver um modelo estatístico que define o limite de tráfego admissível. Entretanto esse modelo pode ser construído de forma estática. Em caso haja um desvio desse comportamento, o processo de mitigação é disparado.
- **Politicas pré-definidas:** Esta técnica funciona a partir da implementação de políticas de segurança previamente estabelecidas pelos administradores da rede, em grande parte estáticas. Em seguida todos os fluxos que chegam ao sistema são submetidos a essas políticas e caso não atendam seus requisitos, serão considerados como maliciosos.
- **Machine Learning:** Os algoritmos presentes nesta categoria utilizam um conjunto de dados de treinamento para se adaptar gradativamente as mudanças ocorridas no sistema e tomar decisões em tempo real a respeito da melhor ação de mitigação que deve ser aplicada com base em diversas situações de ameaças. Entre eles estão: algoritmos genéticos, lógica fuzzy, redes bayesianas, redes neurais e etc.

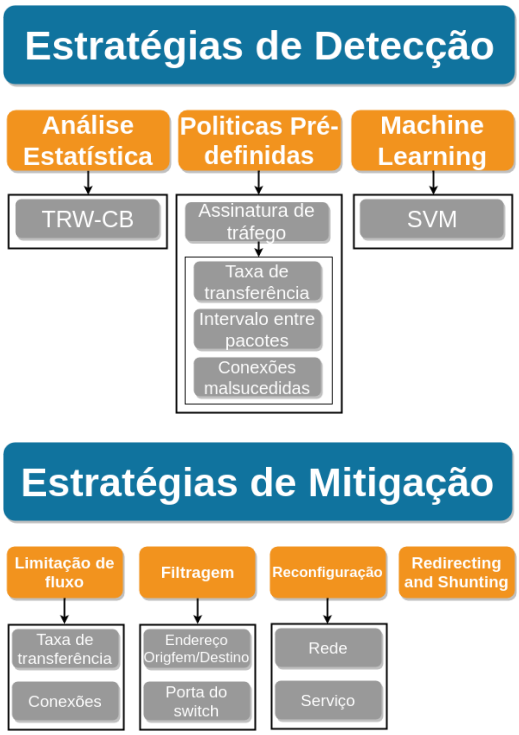

Figura 1. Visão geral das estratégias de detecção e mitigação utilizadas pelas soluções revisadas.

3.2.3. Estratégias de Mitigação

Por fim foi levado em consideração, a estratégia de mitigação empregada em cada solução como critério de classificação. Na figura 1 é apresentada de forma esquematizada um resumo principais estratégias de detecção e mitigação utilizadas. Neste sentido o trabalho desenvolvido em [Shameli-Sendi et al. 2015], também apresenta uma extensa classificação e foi utilizado como base no presente estudo, conforme mostrado abaixo:

- **Limitação de fluxo:** O objetivo desta técnica é descartar a fração de tráfego que excede a capacidade total que o sistema é capaz de lidar, mantendo a disponibilidade do mesmo.
- **Filtragem:** Nesta técnica, é realizado o bloqueio dos pacotes que entram no sistema, com base em uma ou várias características de tráfego previamente selecionadas.
- **Pushback:** Nesta estratégia, diversos domínios colaboram entre si encaminhando as informações referentes a um ataque afim de limitar a taxa de fluxos o mais próximo possível de o mais próximo possível de sua origem.
- **Reconfiguração:** Está técnica pode ser dividida em três grupos principais: *(i)* Reconfiguração de rede, onde a topologia é alterada provendo rotas alternativas para evitar o congestionamento causado pelos ataques DDoS;*(ii)* Reconfiguração de serviço, onde novas instâncias do serviço alvo são criadas em diferentes localizações.
- **Redireting and Shunting:** Nesta técnica os fluxos apontados como maliciosos, ao invés de serem imediatamente descartados são encaminhados para um dispositivo capaz de realizar uma análise mais profunda, com o intuito de extrair informações relevantes e realizar a extração do tráfego malicioso e encaminhando o tráfego benigno em direção ao seu destino final.

4. Soluções de Mitigação de DDoS baseadas em SDN

Os autores em [Bull et al. 2016] propuseram a mitigar diversos ataques DDoS, através da implementação de uma solução baseada em três componentes principais: *(i)* Switches Openflow; *(ii)* Gerenciador de estatísticas e;*(iii)* um conjunto de ações de mitigação. Os switches Openflow são um elemento primordial, atuando no encaminhamento de fluxos para o Gerenciador de estatísticas que irá coletar essas informações e fornecer recursos para que o controlador selecione a melhor ação de mitigação a ser aplicada, que pode ser uma das seguintes: *(i)* Bloquear efetivamente um fluxo ; *(ii)* Encaminhar um fluxo para quarentena para uma análise profunda, antes decidir seu devido tratamento e; *(iii)* Limitar a taxa de fluxo afim de minimizar os impactos causados a rede. Todavia os autores não realizaram uma discussão aprofundada sobre os detalhes de implementação dos mecanismos, como os métodos de classificação que oram empregados para geração dos alertas de ataque. Ademais, a efetividade do mecanismo proposto foi validade no escopo de poucos tipos de ataques DDoS.

O trabalho desenvolvido por [Sharma et al. 2017] apresenta o framework *Dist-BlockNet*, uma arquitetura de segurança distribuída que emprega as tecnologias blockchain e SDN para proteger ambientes IoT. Os autores desenvolveram uma arquitetura modular capaz de prover escalabilidade e flexibilidade excluindo a necessidade de um controlador central, que em muitos casos pode implementar um ponto único de falha. Além disso o framework é capaz de se adaptar automaticamente a diversos cenários de ameaças, como ataques DDoS, envenenamento ARP(ARP Poisoning) e ataques de falsificação de topologia (Fake Topology Attacks). A arquitetura é baseada em dois módulos principais: *(i)* Orchapp e; *(ii)* Shelter. O Orchapp é responsável por implementar dinamicamente as politicas de segurança aplicadas ao sistema. Enquanto o módulo Shelter atua principalmente na camada de dados, coletando informações de tráfego e gerando diagramas com estatísticas de fluxo que são fornecidos ao Orchapp. Após colher essas estatísticas o Or-

chapp irá utilizar um dos mecanismos de detecção disponíveis para verificar a ocorrência de um ataque, e em caso positivo atualizar por meio da técnica de blockchain todas as tabelas de fluxo do sistema com as medidas de segurança mais adequadas. Apesar de ser capaz de selecionar adequadamente politicas de segurança em diferentes cenários de ameaças, o framework depende que as politicas de segurança sejam especificadas pelo administrador da rede, caso contrário não irá funcionar corretamente na contenção de ameaças

[Bhunia and Gurusamy 2017] desenvolveu um framework hierárquico denominado *SoftThings* que assim como o mecanismo revisado anteriormente se propõe a mitigar uma ampla gama de ataques DDoS. Todavia, focando em redes de dispositivos IoT domiciliares. A arquitetura do *SoftThings* é segmentada em quatro subníveis: *(i)* Dispositivos IoT; *(ii)* Switches SDN; *(iii)* Controlador de cluster SDN e; *(iiii)* Controlador SDN mestre. A base da hierarquia é formada por clusters de dispositivos IoT interconectados ao mesmo switch SDN. Para cada cluster é atribuído um Controlador de Cluster SDN responsável pelo seu gerenciamento. Por sua vez cada Controlador de Cluster SDN tem de informar periodicamente o estado de sua rede para o Controlador SDN Mestre que está no topo da hierarquia do *SoftThings* e é responsável por tomadas de decisões globais que serão aplicadas a toda infraestrutura.

O processo de detecção é iniciado quando o Controlador de cluster SDN, reconhece um comportamento anômalo, com base nas estatísticas de tráfego oferecidas pelos switches que monitoram o tráfego dos dispositivo IoT conectado a ele. No Controlador de cluster SDN residem três módulos: *Learning module*, *Classification module* e *Flow Management Module*. O *Learning Module* utiliza as estatísticas de tráfego em condições normais coletadas dos switches OpenFlow e padrões de tráfego de ataque, para continuamente alimentar o *Classification module* com dados de treinamento. O *Classification module* utiliza o algoritmo Support Vector Machine (SVM), para detecção de anomalias e informa ao *Flow management module* que seleciona a medida de segurança apropriada, que pode ser: *(i)* Envio do endereço malicioso para ser adicionado em uma blacklist no Controlador SDN Mestre e; *(ii)* bloqueio total do fluxo malicioso nos switches OpenFlow. Apesar do framework ser focado em garantir escalabilidade, através da existência de diversos controladores para gerenciar clusters de dispositivos SDN o Controlador SDN Mestre representa um ponto único de falha e pode colocar em risco a disponibilidade de toda a infraestrutura.

Em contraste com as abordagens citadas anteriormente, que implementam proteção contra ameaças internas e externas, [Ozcelik et al. 2017] propôs uma solução que se destina unicamente a monitorar o tráfego proveniente de redes IoT, afim de detectar comportamentos anômalos. Segundo os autores quanto mais próximo da fonte, mais eficiente será o processo de detecção e mitigação. O mecanismo implementa pequenas infraestruturas na borda de redes alvos tem a capacidade de analisar todo o tráfego de saída e determinar sua legitimidade. Em caso de fluxos maliciosos, o mecanismos realiza o bloqueio total do tráfego ilegítimo. Para tal fim é utilizado o algoritmo TRW-CB (Threshold Random Walk with Credit Based Rate Limiting) que verificar a legitimidade dos fluxos analisados. Porém o processo de mitigação é desencadeado com base em uma quantidade estática de conexões malsucedidas por segundo. É importante ressaltar que a utilização dessa abordagem pode implicar em um processo de detecção ineficiente, em casos onde o

atacante emite uma pequena quantidade de tráfego, imitando o comportamento de clientes autêntico.

Em [Yin et al. 2018] os autores desenvolveram o framework SD-IoT, e desenvolveram um método de detecção baseado no algoritmo *cosine similarity*. O ponto chave da implementação do algoritmo descrito pelos autores é comparar amostras de pacotes do tipo *Packet-ins* que chegam periodicamente ao controlador com um limite ideal pré-definido. Os autores denominam essas amostras como vetores. A diferença entre os vetores deve ficar abaixo do límite pré-determinado, intitulado de semelhança de cosenos, que representa um valor entre 0 e 1. Caso essa condição não seja alcançada, isso pode indicar que um ataque DDoS está em curso na rede. Em seguida é gerado um alarme para que o processo de mitigação seja disparado. Após a identificação dos fluxos maliciosos o mecanismo identifica qual a porta e switch Openflow de origem dos fluxos e aplica a política de bloqueio. Apesar da eficácia da abordagem proposta, os autores deixam claro que o processo de determinação do valor limite de semelhança é complexo e deve ser feito adequadamente. Pois se esse valor for demasiado alto, parte do tráfego DDoS será classificado como benigno, enquanto que se for muito baixo, pacotes normais serão classificados como maliciosos, comprometendo assim a eficácia do processo de mitigação.

Outra abordagem que empregou gateways SDN para proteger infraestruturas IoT, foi desenvolvida em [Yan et al. 2018] onde foi proposto um framework distribuído denominado MLDMF (multi-level DDoS mitigation framework). Os autores se concentraram em desenvolver uma abordagem escalável e tolerante a falhas. Em função disso o framework é dividido em três camadas principais: *(i)* Computação de borda; *(ii)* Computação em névoa e; *(iii)* Computação em nuvem. A camada de computação de borda está diretamente conectada aos dispositivos IoT é implementada por um gateway SDN responsável principalmente por garantir o controle de acesso, a comunicação de dados segura e a aplicação das medidas de segurança provenientes da camada de computação em névoa, que está em um nível logo acima e tem como tarefa primordial coletar as estatísticas de tráfego e enviá-los para a camada de nuvem no topo da infraestrutura, onde são definidas as politicas de segurança a nível de aplicação que serão aplicadas globalmente. Apesar de se propor a prevenir proativamente diversas ameaças, quando se trata de ataques externos, o mecanismo foi avaliado em cenários de ataques de pequena escala. Portanto, é sugerido também a implementação do mecanismo em cenários críticos, com grandes quantidades de tráfego afim de garantir sua eficácia inclusive nesssas situações.

Seguindo a perspectiva dos dois trabalhos anteriores em [Krishnan et al. 2018] foi implementada uma arquitetura para gerenciamento de redes IoT em larga escala. Provendo segurança e escalabilidade por meio da integração de gateways e controladores SDN na borda de redes IoT. O gerenciamento de alto nível é realizado a partir da camada de nuvem que atua na definição de politicas de segurança e as transmite à camada de névoa para que esta possa aplicá-la aos dispositivos IoT gerenciados na base da infraestrutura. Os autores realizaram um estudo sobre sua utilização na defesa contra ataques DDoS do tipo HTTP Flooding. Para este fim foram utilizados um switch SDN conectado a um dispositivo executando uma aplicação HTTP. Foi instalada uma regra de fluxo no switch, que disparava um alerta de ataque, caso o número de tentativas de conexão ao servidor excedesse o limite de 350 tentativas por segundo. Após a comprovação do ataque todas conexões ilegítimas são descartadas e uma mensagem de redirecionamento de endereço

do servidor é enviada para todos os clientes. Caso algum cliente mal-intencionado receba a mensagem, espera-se que ele não seja capaz de decodificá-la, continuando o ataque ao endereço original. Apesar de desenvolverem uma abordagem capaz de prover segurança em ambientes IoT de larga escala, a utilização de mecanismos pouco flexíveis, dificulta a aplicabilidade da solução em ambientes heterogêneos.

No trabalho desenvolvido em [Sharma et al. 2018] foi proposta uma arquitetura genérica modular denominada *ShSec*, que atua como um middleware, provendo segurança em casas inteligentes. A arquitetura oferece prevenção a incidentes internos e externos, atuando na integração entre as camadas de aplicação e dados SDN. O mecanismo é composto por dois componentes principais: *(i)* Orchestrator e; *(ii)* KNOT. O módulo Orchestrator é responsável por manter interoperabilidade entre a camada de aplicação SDN e a arquitetura ShSec, provendo comunicação de dados confiável. Enquanto que o módulo KNOT implementa as funções de proteção contra ameaças de rede. Sempre que um novo fluxo chega ao controlador na camada de aplicação, o gráfico de fluxo da rede é atualizado e é realizada uma checagem ao banco de dados de ataques, para constatar se os fluxos correspondem a um ataque conhecido. Caso positivo o controlador irá gerar um alarme e instalar a política de bloqueio adequada, para realizar a mitigação dos fluxos maliciosos. Caso negativo o fluxo é enviado para uma inspeção mais profunda, afim de atualizar o banco de dados de ataque conhecidos. Apesar de se propor a prevenir proativamente diversas ameaças, quando se trata de ataques externos, o mecanismo foi avaliado em cenários de ataques de pequena escala. Portanto, assim como no trabalho desenvolvido em [Yan et al. 2018] também é necessária a implementação do presente framework em cenários de larga escala, afim de avaliar sua eficácia nessas situações.

Em [Salva-Garcia et al. 2018] e [Molina Zarca et al. 2018] foi apresentado um framework distribuído de segurança utilizando mecanismos filtragem de tráfego para fornecer funcionalidades de controle de acesso e gerenciamento em redes de dispositivos IoT, fazendo uso da integração das tecnologias SDN e NFV. A abordagem implementa politicas de filtragem, que são proativamente especificadas pelo administrador da rede utilizando uma interface gráfica de suporte localizada na camada de administração no topo da arquitetura. Em seguida essas politicas são traduzidas em configurações de baixo nível e o plano de orquestração de segurança se encarrega de encaminhá-las ao plano de execução de segurança, aqui implementado por diversos gateways SDN, residindo na borda da rede de destino. Em cada um desses gateways SDN residem agentes de filtragem e monitoramento responsáveis pelo processo de detecção e mitigação de ameaças. O agente de monitoramento realiza a confirmação da existência de um ataque DDoS utilizando como base um banco de dados de assinaturas de ataques pré-configuradas. Em seguida, caso os fluxos coincidam com um dos padrões é disparado um alarme para o agente de filtragem, que irá reagir bloqueando todos os fluxo maliciosos. Apesar da arquitetura ser capaz de prover segurança em ambientes IoT, a necessidade manual de atualizações das politicas de filtragem pelo administrador da rede, torna necessário a especificação de mecanismos mais flexíveis e auto gerenciáveis.

5. Classificação das Soluções

A tabela 2 apresenta as soluções de mitigação descritas na seção anterior, classificadas com base na taxonomia proposta. Comumente, ataques DDoS geram uma quantidade significativa de tráfego na rede. Portanto, uma ideia natural para detectar tais ataques é

identificar variações abruptas no volume de tráfego da rede. Nesse sentido, pode-se observar que a maioria das soluções (70%) adota métodos estatísticos para modelar o fluxo de tráfego normal da rede. Se o comportamento observado desviar significativamente desse modelo, então suspeita-se que o sistema está sob ataque. Alguns autores aplicam um limiar estático para distinguir uma situação de ataque de uma situação real, enquanto que outros adotam um limiar dinâmico para refletir as variações do padrão de tráfego que podem ocorrer em diferentes períodos do dia. Uma limitação do uso de limiar estático é que a defesa precisa passar por uma etapa de treinamento antes de realmente ser testada em uma situação real. Um limiar dinâmico pode ser enganado por atacantes inteligentes que expandem gradualmente o tráfego do ataque, aumentando o limiar para acompanhar o aparente crescimento do tráfego legítimo.

Solução	Detecção	Mitigação	Localização	Limitações
[Bull et al. 2016]	Análise estatística	Filtragem, Redirecting and Shunting, Limitação de fluxo.	Borda da rede	Os autores não especificam com profundidade os detalhes de implementação do mecanismo de detecção; Validação com poucos ataques.
[Sharma et al. 2017]	Políticas pré-definidas	Filtragem	Distribuída	Os autores não especificam com profundidade os detalhes de implementação do mecanismo de detecção e mitigação.
[Bhunia and Gurusamy 2017]	Machine Learning	Filtragem e Limitação de Fluxo	Distribuída	O Master SDN Controller implementa um ponto único de falha, impactando na disponibilidade de toda a infraestrutura
[Ozcelik et al. 2017]	Análise estatística	Filtragem	Distribuída	Detecção baseado em parâmetros estáticos.
[Yin et al. 2018]	Análise estatística	Filtragem	Distribuída	O cálculo do valor ideal de similaridade de cosenos é complexo e impacta negativamente na eficiência do mecanismo, caso não seja feita adequadamente.
[Yan et al. 2018]	Análise estatística	Filtragem	Distribuída	Mecanismo não avaliado em cenários de ataques de larga escala.
[Krishnan et al. 2018]	Análise estatística	Reconfiguração	Distribuída	Detecção baseada em parâmetros estáticos.
[Sharma et al. 2018]	Análise estatística	Filtragem, Redirecting and Shunting	Borda da rede	Mecanismo não avaliado em cenários de ataques de larga escala.
[Salva-Garcia et al. 2018]	Políticas pré-definidas	Filtragem	Distribuída	Necessidade de atualização manual das politicas de filtragem.

Tabela 2. Sumário das soluções de mitigação de ataques DDoS usando SDN, aplicadas a ambientes IoT.

No que diz respeito as ações mitigadoras de risco, a filtragem de tráfego é empregada com uma maior frequência. Embora essa defesa possa ser eficaz na mitigação de casos específicos de um ataque, dentre suas desvantagens destaca-se o fato de que muitas soluções assumem que um endereço IP esta associado a um único cliente. No entanto, tal hipótese não pode ser mantida quando vários clientes são multiplexados por trás de um NAT ou proxy. Um ataque realizado por poucos clientes mal-intencionados pode resul-

tar no bloqueio do serviço para todas as solicitação por trás do endereço IP do roteador NAT ou proxy, impedindo que outros usuários honestos usem o serviço. Por fim, foi observado que cerca de 80% das soluções implementam frameworks distribuídos em várias camadas para prover maior escalabilidade e flexibilidade. Entretanto cada camada pode se tornar um alvo em potencial dos atacantes, influenciando na disponibilidade de toda infraestrutura.

Portanto, é possível concluir que a detecção e mitigação de ataques DDoS baseados em IoT continua sendo um tema de pesquisa relevante e desafiador e que a tecnologia SDN deve ser melhor explorada para prover uma soluções mais robusta contra esses ataques.

6. Conclusão

Neste trabalho foi proposta uma taxonomia das principais soluções existentes de defesa contra ataques DDoS usando o paradigma SDN em ambientes IoT. Isso foi viabilizado mediante a definição de critérios capazes de auxiliar na compreensão das contribuições oferecidas pelas abordagens revisadas. Adicionalmente foi apresentada uma classificação satisfatória das estratégias de detecção e mitigação empregadas em cada solução. Por fim, com base nos resultados obtidos foi comprovada a eficacia do paradigma SDN, como um meio de proteger ambientes IoT contra ataques DDoS.

Todavia ainda existem questionamentos em aberto como: *(i)* A própria segurança da infraestrutura SDN, diante de ameaças de alto risco, como os ataques DDoS e; *(ii)* Aplicabilidade em cenários reais das soluções de mitigação desenvolvidas. Estes questionamentos serão abordados em uma taxonomia futura que irá abranger um maior número de critérios de classificação e soluções.

7. Agradecimentos

Esta pesquisa foi parcialmente apoiada pela 4ª chamada colaborativa EU-BR (H2020, *grant agreement* no. 777067, NECOS – *Novel Enablers for Cloud Slicing*), financiada pela Comissão Européia e pelo Ministério da Ciência, Tecnologia, Inovação e Comunicação (MCTIC), através da RNP e CTIC. Os autores também agradecem ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e ao IFRN pelo apoio.

Referências

[Al-Fuqaha et al. 2015] Al-Fuqaha, A. I., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys and Tutorials*, 17(4):2347–2376.

[Bertino and Islam 2017] Bertino, E. and Islam, N. (2017). Botnets and internet of things security. *Computer*, 50(2):76–79.

[Bhunia and Gurusamy 2017] Bhunia, S. S. and Gurusamy, M. (2017). Dynamic attack detection and mitigation in iot using sdn. In *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, pages 1–6.

[Bull et al. 2016] Bull, P., Austin, R., Popov, E., Sharma, M., and Watson, R. (2016). Flow based security for iot devices using an sdn gateway. In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pages 157–163.

[Ceron et al. 2016] Ceron, J. M., Margi, C. B., and Granville, L. Z. (2016). Mars: An sdn-based malware analysis solution. In *2016 IEEE Symposium on Computers and Communication (ISCC)*, pages 525–530.

[Cherian and Chatterjee 2019] Cherian, M. and Chatterjee, M. (2019). Survey of security threats in iot and emerging countermeasures. In Thampi, S. M., Madria, S., Wang, G., Rawat, D. B., and Alcaraz Calero, J. M., editors, *Security in Computing and Communications*, pages 591–604, Singapore. Springer Singapore.

[Dayal et al. 2016] Dayal, N., Maity, P., Srivastava, S., and Khondoker, R. (2016). Research trends in security and ddos in sdn. *Security and Communication Networks*, 9(18):6386–6411.

[Farris et al. 2019] Farris, I., Taleb, T., Khettab, Y., and Song, J. (2019). A survey on emerging sdn and nfv security mechanisms for iot systems. *IEEE Communications Surveys Tutorials*, 21(1):812–837.

[Kalkan et al. 2017] Kalkan, K., Gur, G., and Alagoz, F. (2017). Defense mechanisms against ddos attacks in sdn environment. *IEEE Communications Magazine*, 55(9):175–179.

[Kalkan and Zeadally 2018] Kalkan, K. and Zeadally, S. (2018). Securing internet of things with software defined networking. *IEEE Communications Magazine*, 56(9):186–192.

[Kanagavelu and Aung 2019] Kanagavelu, R. and Aung, K. M. M. (2019). A survey on sdn based security in internet of things. In Arai, K., Kapoor, S., and Bhatia, R., editors, *Advances in Information and Communication Networks*, pages 563–577, Cham. Springer International Publishing.

[Kolias et al. 2017] Kolias, C., Kambourakis, G., Stavrou, A., and Voas, J. (2017). Ddos in the iot: Mirai and other botnets. *Computer*, 50(7):80–84.

[Koufopavlou 2015] Koufopavlou, E. H. K. P. S. D. J. H. S. D. M. O. (2015). Software-Defined Networking (SDN): Layers and Architecture Terminology. RFC 7426.

[Kouicem et al. 2018] Kouicem, D. E., Bouabdallah, A., and Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, 141:199 – 221.

[Krishnan et al. 2018] Krishnan, P., Najeem, J. S., and Achuthan, K. (2018). Sdn framework for securing iot networks. In Kumar, N. and Thakre, A., editors, *Ubiquitous Communications and Network Computing*, pages 116–129, Cham. Springer International Publishing.

[Lohachab and Karambir 2018] Lohachab, A. and Karambir, B. (2018). Critical analysis of ddos—an emerging security threat over iot networks. *Journal of Communications and Information Networks*, 3(3):57–78.

[Marzano et al. 2018] Marzano, A., Alexander, D., Fonseca, O., Fazzion, E., Hoepers, C., Steding-Jessen, K., Chaves, M. H. P. C., Cunha, , Guedes, D., and Meira, W. (2018). The evolution of bashlite and mirai iot botnets. In *2018 IEEE Symposium on Computers and Communications (ISCC)*, pages 00813–00818.

[Molina Zarca et al. 2018] Molina Zarca, A., Bernal Bernabe, J., Farris, I., Khettab, Y., Taleb, T., and Skarmeta, A. (2018). Enhancing iot security through network softwariza-

tion and virtual security appliances. *International Journal of Network Management*, 28(5):e2038. e2038 nem.2038.

[Noor and Hassan 2019] Noor, M. and Hassan, H. (2019). Current research on internet of things (iot) security: A survey. *Computer Networks*, 148:283–294.

[Ozcelik et al. 2017] Ozcelik, M., Chalabianloo, N., and Gür, G. (2017). Software-defined edge defense against iot-based ddos. In *2017 IEEE International Conference on Computer and Information Technology (CIT)*, pages 308–313.

[Salva-Garcia et al. 2018] Salva-Garcia, P., Alcaraz-Calero, J. M., Wang, A., Qi, B., Bernal, J., and Skarmeta, A. (2018). 5g nb-iot: Efficient network traffic filtering for multitenant iot cellular networks. *Security and Communication Networks*.

[Shameli-Sendi et al. 2015] Shameli-Sendi, A., Pourzandi, M., Fekih-Ahmed, M., and Cheriet, M. (2015). Taxonomy of distributed denial of service mitigation approaches for cloud computing. *Journal of Network and Computer Applications*, 58:165 – 179.

[Sharma et al. 2018] Sharma, P. K., Park, J. H., Jeong, Y.-S., and Park, J. H. (2018). Shsec: Sdn based secure smart home network architecture for internet of things. *Mobile Networks and Applications*.

[Sharma et al. 2017] Sharma, P. K., Singh, S., Jeong, Y., and Park, J. H. (2017). Distblocknet: A distributed blockchains-based secure sdn architecture for iot networks. *IEEE Communications Magazine*, 55(9):78–85.

[Shi et al. 2017] Shi, Y., Dai, F., and Ye, Z. (2017). An enhanced security framework of software defined network based on attribute-based encryption. In *2017 4th International Conference on Systems and Informatics (ICSAI)*, pages 965–969.

[Yakasai and Guy 2015] Yakasai, S. T. and Guy, C. G. (2015). Flowidentity: Software-defined network access control. In *2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN)*, pages 115–120.

[Yan et al. 2018] Yan, Q., Huang, W., Luo, X., Gong, Q., and Yu, F. R. (2018). A multi-level ddos mitigation framework for the industrial internet of things. *IEEE Communications Magazine*, 56(2):30–36.

[Yan et al. 2016] Yan, Q., Yu, F. R., Gong, Q., and Li, J. (2016). Software-defined networking (sdn) and distributed denial of service (ddos) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Communications Surveys Tutorials*, 18(1):602–622.

[Yin et al. 2018] Yin, D., Zhang, L., and Yang, K. (2018). A ddos attack detection and mitigation with software-defined internet of things framework. *IEEE Access*, 6:24694–24705.

[Zargar et al. 2013] Zargar, S. T., Joshi, J., and Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. *IEEE Communications Surveys Tutorials*, 15(4):2046–2069.