Inteligência artificial para identificar e tratar ataques DDoS em redes baseadas em SDN: Revisão sistemática.

Lucas Ribeiro Machado

Resumo

Introdução: O artigo visa explorar a relação entre a Inteligência Artificial (IA) e os ataques de negação de serviço distribuídos (DDoS) em redes baseadas em SDN. O objetivo é compreender como a IA pode aperfeiçoar e agravar as ameaças cibernéticas, desenvolvendo estratégias avançadas de defesa e detecção de ataques para contribuir para um ambiente digital mais seguro e resiliente na área de Sistemas da Informação. Além disso, destaca-se a importância da IA na simulação da inteligência humana e no aprendizado de máquina para lidar com grandes conjuntos de dados e melhorar suas habilidades ao longo do tempo. ***Metodologia:*** O estudo baseou-se nas características da revisão sistemática, seguindo as diretrizes PRISMA. Foram utilizados critérios de inclusão e exclusão para a seleção dos artigos, considerando a relação entre a IA e a detecção de ataques DDoS, a menção das palavras-chave no título, a abordagem dos ataques DDoS e a publicação entre 2019 e 2023. O processo de seleção dos artigos consistiu na triagem do título, resumo e texto completo, resultando na seleção de 11 artigos relevantes para a pesquisa. ***Resultados:*** A análise global do processo de seleção dos estudos resultou na identificação de 11 artigos relevantes para a pesquisa, destacando a importância da IA na detecção de ataques DDoS nos dias atuais. Além disso, ressalta-se a necessidade de abordagens holísticas e adaptativas para a detecção eficaz dos ataques DDoS, considerando as características específicas das redes e a escolha de técnicas e ferramentas promissoras para atender às necessidades das organizações. ***Conclusão:*** O estudo conclui que não existe um método determinado ou "melhor" para a detecção de ataques DDoS, sendo a eficácia da detecção dependente de diversos fatores, como o tipo de ataque, o tipo de rede e os recursos disponíveis.

Abstract

Introduction: The article aims to explore the relationship between Artificial Intelligence (AI) and distributed denial of service (DDoS) attacks in SDN-based networks. The objective is to understand how AI can improve and aggravate cyber threats, developing advanced defense and attack detection strategies to contribute to a safer and more resilient digital environment in the area of Information Systems. Furthermore, the importance of AI in simulating human intelligence and machine learning to deal with large data sets and improve its skills over time is highlighted. **Methodology:** The study was based on the characteristics of the systematic

review, following the PRISMA guidelines. Inclusion and exclusion criteria were used to select the articles, considering the relationship between AI and the detection of DDoS attacks, the mention of keywords in the title, the approach to DDoS attacks and publication between 2019 and 2023. The process The article selection process consisted of screening the title, abstract and full text, resulting in the selection of 11 articles relevant to the research. **Results:** The global analysis of the study selection process resulted in the identification of 11 articles relevant to the research, highlighting the importance of AI in detecting DDoS attacks today. Furthermore, the need for holistic and adaptive approaches for the effective detection of DDoS attacks is highlighted, considering the specific characteristics of networks and the choice of promising techniques and tools to meet the needs of organizations. **Conclusion:** The study concludes that there is no determined or "best" method for detecting DDoS attacks, with the effectiveness of detection depending on several factors, such as the type of attack, the type of network and the available resources.

Palavras-chave: *Machine Learning, Attacks DDoS, SDN Networks.*

1. Introdução

A Inteligência Artificial (IA) é uma área da ciência da computação que busca desenvolver sistemas capazes de realizar tarefas que, até então, eram exclusivas da inteligência humana. Com o avanço tecnológico e a crescente disponibilidade de dados, a IA tem se tornado uma das tecnologias mais transformadoras do nosso tempo, encontrando aplicação em diversas áreas, desde assistentes virtuais até diagnósticos médicos precisos (RODRIGUES et al., 2020).

Assim como ocorreu com outras tecnologias que representaram grande avanço para a sociedade, a IA também pode vir a ser usada com propósitos maliciosos. Um exemplo significativo é a ocorrência cada vez mais frequente de ataques de negação de serviço (DDoS, do inglês Distributed Denial of Service). Esses ataques visam sobrecarregar um sistema ou rede com um volume massivo de tráfego, impossibilitando o acesso de usuários legítimos e, em alguns casos, causando danos consideráveis às organizações afetadas (WANG et al., 2019).

A relação entre a Inteligência Artificial e os ataques DDoS reside na utilização cada vez mais sofisticada de técnicas de IA pelos cibercriminosos

para aprimorar suas estratégias de ataque. A capacidade da IA de analisar grandes volumes de dados e identificar padrões possibilita a criação de botnets mais inteligentes e automatizadas, capazes de se adaptar às defesas de maneira mais eficiente. Além disso, a IA permite a detecção de vulnerabilidades em tempo real, o que potencializa a eficácia e a escala dos ataques.

A importância de compreender essa relação é crucial para a área de Sistemas da Informação, visto que a proteção contra-ataques DDoS é essencial para garantir a continuidade e a segurança das operações das organizações no ambiente digital. Como destacado por Rodrigues et al. (2020), os ataques DDoS são um dos principais desafios enfrentados pelas equipes de segurança cibernética, exigindo uma abordagem proativa e atualizada para mitigar seus impactos.

Compreender as táticas empregadas pelos cibercriminosos, aliadas às capacidades da IA, permite que profissionais de Sistemas da Informação desenvolvam estratégias de defesa mais robustas e eficientes. Além disso, a investigação de métodos inovadores que utilizam a IA para a detecção precoce e a mitigação de ataques DDoS pode trazer uma nova perspectiva para o campo da segurança cibernética, como afirmado por Wang et al. (2019).

Em síntese, este trabalho visa explorar a relação entre a Inteligência Artificial e os ataques DDoS, compreendendo como a utilização da IA pode aperfeiçoar e agravar as ameaças cibernéticas. Através dessa compreensão, espera-se que sejam desenvolvidas estratégias avançadas de defesa e detecção de ataques, contribuindo para um ambiente digital mais seguro e resiliente para a área de Sistemas da Informação.

2. Revisão de Literatura

2.1. Inteligencia Artificial

A inteligência artificial (IA) é um campo da ciência da computação que busca desenvolver sistemas e máquinas capazes de simular a inteligência humana. A ideia por trás da IA é criar programas e algoritmos que possam realizar tarefas que normalmente exigiriam habilidades cognitivas humanas, como aprendizado, raciocínio, resolução de problemas, compreensão de linguagem natural, reconhecimento de padrões e tomada de decisões (COSSETTI, 2018).

A IA procura entender como os seres humanos pensam, aprendem e processam informações para replicar esses processos em máquinas. Por meio da coleta e análise de grandes conjuntos de dados, algoritmos de aprendizado de máquina permitem que os sistemas de IA aprendam com exemplos passados e melhorem suas próprias habilidades ao longo do tempo (LUDERMIR et al., 2021).

Existem várias abordagens para alcançar a inteligência artificial. Uma delas é o aprendizado de máquina, que permite que os computadores "aprendam" a partir de dados e façam previsões ou tomem decisões com base nesse aprendizado. Outra abordagem é o uso de redes neurais artificiais, que são sistemas que imitam o funcionamento do cérebro humano para resolver problemas complexos, um exemplo seria a possibilidade de hoje em dia existir carros que dirigem sozinhos, tais como o Tesla ou os carros do Google (FENG et al., 2021). A IA tem o potencial de revolucionar várias indústrias, melhorar a eficiência e a precisão de tarefas e até mesmo criar novos produtos e serviços que antes não eram possíveis. De algum tempo para cá, a IA teve que evoluir no poder computacional para ganhar ainda mais espaço no mundo atual. No entanto, a IA também traz desafios e questões éticas importantes. A privacidade dos dados, o viés algorítmico, a responsabilidade por decisões automatizadas e o impacto no mercado de trabalho são algumas das preocupações que devem ser consideradas ao desenvolver e implementar sistemas de inteligência artificial.

Existem três categorias de IA podendo ser caracterizada como IA Focada, na qual algoritmos especializados resolverão problemas específicos; IA Generalizada, que os algoritmos são capazes de realizar tarefas humanas, utilizando muitas vezes o Aprendizado de Máquina como ferramenta; ou IA Superinteligente onde os algoritmos são mais capazes que os próprios humanos para executar tarefas (LUDERMIR et al. 2021).

O Aprendizado de Máquina (ML) tem um papel importante na IA, já que possui o objetivo de construir programas que melhorem o desempenho dos dados computacionais (MITCHELL et al., 1997). Os tipos de ML podem se dividir na categoria Aprendizado

Supervisionado, onde é preciso apresentar respostas desejadas a cada modelo informado; Aprendizado Não Supervisionado, que não é fornecido rótulos a serem seguidos, pois o algoritmo irá se basear em exemplos similares aos atributos cedidos; ou Aprendizado por Reforço, na qual o algoritmo não recebe uma resposta correta, entretanto recebe um sinal de reforço, recompensa ou punição (LUDERMIR et al. 2021).

Em resumo, a inteligência artificial é um campo empolgante e em constante evolução, que busca capacitar as máquinas com habilidades humanas para tornar nossas vidas mais eficientes e convenientes. Embora ainda haja muito a ser explorado e aprimorado, o potencial da IA para moldar o futuro é promissor e inspirador.

2.2. Ataques DDoS

Um Ataque de Negação de Serviço Distribuído, do inglês DDoS - Distributed Denial of Service, é uma forma de ataque cibernético que tem o objetivo de tornar um serviço, site ou recurso online inacessível aos usuários legítimos, sobrecarregando-o com um volume massivo de tráfego malicioso. Os ataques DDoS ocorrem por indivíduos mal-intencionados, grupos hackers, organizações criminosas ou até mesmo por motivos políticos. Eles geralmente aproveitam uma grande quantidade de dispositivos comprometidos, formando uma "botnet. Diferentemente de um ataque de negação de serviço (DoS) tradicional, no qual um único dispositivo é usado para inundar o serviço-alvo (GONÇALVES, 2018).

Uma botnet é uma rede de dispositivos comprometidos, conhecidos como "bots", que são controlados remotamente por um atacante. Esses bots são frequentemente infectados por malware, permitindo ao invasor executar operações maliciosas sem o conhecimento dos proprietários dos dispositivos. As botnets são usadas para uma variedade de atividades, incluindo ataques de negação de serviço distribuído (DDoS), distribuição de spam, roubo de informações e outras atividades cibernéticas maliciosas. O controle centralizado oferece ao atacante poder de processamento e largura de banda escalava, tornando as botnets uma ameaça significativa para a segurança cibernética. A detecção e prevenção de botnets são desafios constantes na área de segurança online.

Essa botnet é composta por computadores infectados com malware, os quais são controlados remotamente pelo atacante. A partir do momento que o ataque é iniciado, todos os computadores comprometidos dentro da botnet começam a enviar simultaneamente uma grande quantidade de solicitações de acesso ao serviço-alvo. Esse excesso de tráfego, normalmente muito acima da capacidade normal de processamento do serviço, acaba por sobrecarregar os recursos disponíveis, resultando em uma queda ou inoperância completa do serviço (TÉLLEZ et al., 2021).

Os ataques DDoS podem ser conduzidos por diversos motivos, como extorsão, retaliação, ativismo ou até mesmo competição desleal. Eles podem afetar uma ampla gama de alvos, incluindo sites de empresas, instituições financeiras, órgãos governamentais e plataformas online em geral. Existem inúmeros tipos de ataque DDoS, entretanto, os tipos Flood e POD são os mais comuns.

Ataques Flood podem ser amplificados se dependendo da formatação do ataque, já que este acaba se diversificando em vários modelos como o UDP Flood, NTP Flood, SYN Flood ou VolP Flood. O UDP Flood é conhecido como um ataque aleatório precisando apenas de um alvo que possua o pacote UDP, na qual é responsável pela comunicação de muitos pacotes com informações que necessitam de respostas rápidas e o VolP Flood, que trabalha como uma variação do UDP, envia grande quantidade de solicitações falsas para IPs diferentes, tal como o modelo POD. O SYN Flood ocorre quando os próprios atacantes enviam pacotes SYN ao destino. Já o meio NTP Flood é um ataque com pacotes falsificados, porém válidos, com destino a determinado alvo (GONÇALVES, 2018).

A sofisticação dos ataques DDoS tem aumentado ao longo do tempo, tornando-os ainda mais desafiadores de serem mitigados. Os atacantes utilizam várias técnicas, como amplificação de tráfego através de servidores mal configurados, uso de botnets com milhares de dispositivos e até mesmo ataques de reflexão para ampliar o impacto do ataque.

Para proteger-se contra os ataques DDoS, as organizações precisam empregar diversas

estratégias e ferramentas de mitigação, tais como balanceamento de carga, serviços de CDN (Content Delivery Network), sistemas de detecção e prevenção de intrusão (IDPS) e filtros de tráfego. A colaboração com provedores de serviços de internet (ISPs) também pode ser essencial para bloquear o tráfego malicioso antes que ele chegue ao servidor-alvo (CARMENATES et al., 2019).

Em suma, os ataques DDoS são uma ameaça significativa para a disponibilidade e segurança dos serviços online. À medida que a tecnologia continua a evoluir, é importante que as organizações estejam preparadas com soluções robustas para lidar com essas ameaças em constante mudança.

3. Metodologia

3.1. Tipo de Estudo

O presente estudo baseou-se sob as características da revisão sistemática, seguindo as diretrizes PRISMA, que é uma lista de checagem para relatar estudos para revisões sistemáticas e meta-análises, por motivos de haver grande falha ao definir padrões quando se trata de qual seria o melhor meio para detectar os ataques DDoS. Esta metodologia, considerada muito utilizada para responder lacunas relacionadas aos novos estudos, necessita de certa quantidade de dados científicos para o desenvolvimento dos relatos da pesquisa (PRISMA, 2020).

3.2. Busca de Artigos

Por se tratar de um tema recente e em constante atualização foi feita a opção pelo uso de artigos apenas em língua inglesa. Assim, foi utilizado na pesquisa a plataforma de dados Periódicos CAPES. As strings de busca utilizadas na plataforma foram: Machine Learning AND DDoS Attack, DDoS Attack AND SDN Networks, DDoS Attack AND Machine Learning AND SND Networks.

As palavras ao serem inseridas na base de pesquisas foram separadas pelos operadores booleanos “AND” e “OR”, limitando a seleção aos artigos publicados nos últimos 5 anos.

3.3. Critérios de Inclusão e Exclusão

I1. Relação entre a inteligência artificial na detecção de ataques DDoS;

I2. Obter no título a menção das palavras chaves;

I3. Tratar de ataques DDoS;

I4. Publicados entre 2019 e 2023.

E1. Artigos duplicados;

E2. Sem relação da inteligência artificial com os ataques DDoS;

E3. Sem menção a ataques DDoS.

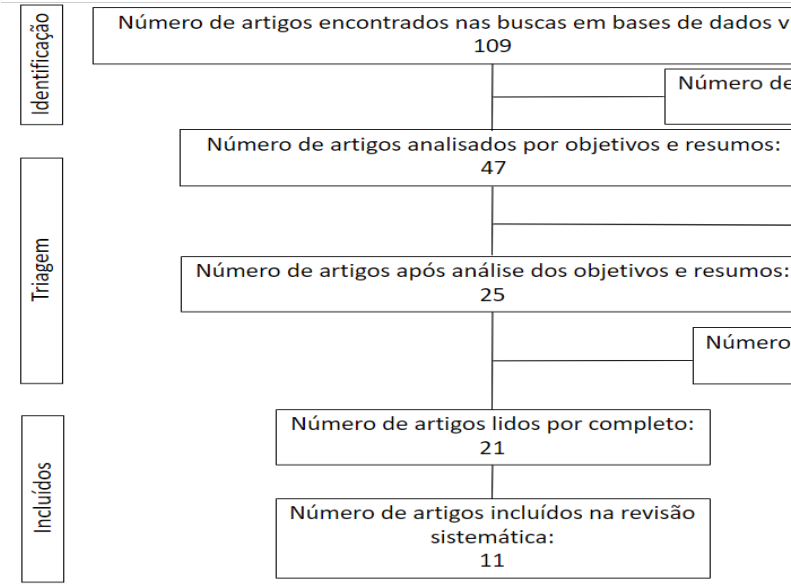
3.4. Seleção dos Artigos

O processo de seleção dos artigos consistiu na triagem do título, resumo e texto completo. Inicialmente os estudos encontrados foram avaliados pelo título, sendo selecionados aqueles que estivessem de acordo com os critérios de inclusão, e excluíram-se os duplicados. Então, foi feita a leitura do resumo, e novamente excluídos os estudos que não relacionaram com o tema proposto. Foi extraído de cada estudo: revista, título, referências, objetivos gerais, metodologia, resultados e conclusão.

4. Resultados e Discussão

4.1 Análise Global

A Figura 1 mostra o processo de seleção da busca pelos estudos utilizando as palavras-chaves. Foram encontrados no total 109 artigos, dos quais foram analisados pela relação do título com o tema da pesquisa. Para analisar os objetivos e resumos foram selecionados 47 artigos, onde logo após restaram apenas 25 artigos e em seguida foram excluídos 4 artigos por cópia, ficando 21 artigos para serem lidos e analisados por completo, mas somente 11 artigos foram determinados como relevantes para a pesquisa. Na Figura 2 é possível identificar a tabela relatando o ano, a revista publicada e o título em sua versão original dos 11 artigos estudados.



Ano	Revista	Título	Metodologia	Nível de Eficácia
2019	ArXiv News	Machine-Learning Techniques for Detecting Attacks in SDN	Análise comparativa das técnicas existentes de aprendizado de máquina para a detecção de tráfego malicioso em SDN.	Aprendizagem Profunda = Eficaz
2020	Journal of King Saud University	A machine learning based attack detection and mitigation using a secure SaaS framework	Foi realizado um processo de detecção de ataques que ocorre em Deep Belief Network (DBN), no qual o peso, bem como a função de ativação, é ajustado com o algoritmo Sea Lion Optimization(MFSLnO) orientado para Median Fitness.	MFSLnO Aprimorado = 89% eficaz
	Electronics - MDPI	A DDoS Attack Mitigation Scheme in ISP Networks Using Machine Learning Based on SDN	Foi proposto uma nova mitigação de ataques DDoS em redes de provedores de serviços de Internet (ISP) baseadas em SDN para ataques de inundação TCP-SYN e ICMP utilizando abordagem de aprendizado de máquina, ou seja, K -Nearest-Neighbor (KNN) e XGBoost.	Aprendizado de Máquinas em Redes = 98% eficaz
	Sustainability - MDPI	Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models	Neste estudo, os ataques DDoS em SDN foram detectados usando modelos baseados em aprendizado de máquina. Foram treinados e testados com modelos de classificação Support Vector Machine (SVM), Naïve Bayes (NB), Rede Neural Artificial (ANN) e K-Nearest Neighbors (KNN).	Aprendizado de Máquinas = >80%
2021	IEEE Access	Detection and Classification of DDoS Flooding Attacks on Software-Defined Networks: A Case Study for the Application of Machine Learning	Neste artigo, a detecção e classificação de ataques de inundação DDoS em SDNs baseadas em aprendizado de máquina são investigadas usando algoritmos populares de aprendizado de máquina (ML). Os algoritmos, classificadores e métodos de ML investigados são análise discriminante quadrática (QDA), Gaussian Naïve Bayes (GNB), k-vizinho mais próximo (k-NN) e árvore de classificação e regressão (CART).	CART = 98% eficaz
	Electronics - MDPI	Machine Learning Approach Equipped with Neighbourhood Component Analysis for DDoS Attack Detection in Software-Defined Networking	Lidamos com um "conjunto de dados SDN de ataque DDoS" público, incluindo um total de 23 recursos. O conjunto de dados consiste em tráfegos normais e de ataque do Protocolo de Controle de Transmissão (TCP), Protocolo de Datagrama do Usuário (UDP) e Protocolo de Mensagens de Controle da Internet (ICMP).	Decision Tree = 100% eficaz
2022	Engineering Science and Technology	Detecting flooding DDoS attacks in software defined networks using supervised learning techniques	Analisamos e comparamos o desempenho, usando diferentes técnicas de ML, para detectar ataques DDoS em SDN, onde são avaliados conjuntos de dados experimentais e dados de tráfego autogerados. Além disso, propomos um modelo simples de aprendizagem supervisionada (SL) para detectar ataques DDoS de inundação contra o controlador SDN através da flutuação de fluxos.	Bagging Tree = 99,64% eficaz
	Sensors - MDPI	Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT	Propomos uma estrutura de detecção e mitigação de ataques distribuídos de negação de serviços (AMLSDM) habilitada para SDN, baseada em aprendizado de máquina adaptativo.	AMLSDM = Válido
	Sensors - MDPI	Review of Botnet Attack Detection in SDN-Enabled IoT Using Machine Learning	Inicialmente, os primeiros grandes ataques de botnets em redes SDN-IoT foram exaustivamente discutidos. Em seguida, são discutidas técnicas de aprendizado de máquina comumente usadas para detectar e mitigar ataques de botnets em redes SDN-IoT. Por fim, o desempenho dessas técnicas de aprendizado de máquina na detecção e mitigação de ataques de botnets é apresentado em termos de métricas de desempenho de modelos de aprendizado de máquina comumente usados.	Aprendizado de Máquinas = Válido
2023	ArXiv News	Detection of DDoS Attacks in Software Defined Networking Using Machine Learning Models	Neste artigo, é investigada a eficácia do uso de algoritmos de aprendizado de máquina para detectar ataques distribuídos de negação de serviço (DDoS) em ambientes de redes definidas por software (SDN). Quatro algoritmos, incluindo Random Forest, Decision Tree, Support Vector Machine e XGBoost, foram testados no conjunto de dados CICDDoS2019, com o recurso de carimbo de data/hora eliminado, entre outros.	Random Forest = 68,9% eficaz
	IEEE Access		Aplicamos a estrutura proposta a três casos de teste: um caso de teste de ataque de nó único e dois casos de teste de ataque de vários nós, todos com tráfego real de IoT gerado e implantado em Mininet-IoT. A estrutura FMDADM proposta detecta com eficiência ataques DDoS em taxas altas e baixas, pode discriminar entre tráfego de ataque e multidões de flash e protege nós de IoT locais e remotos, evitando que a infecção se propague ao nível do ISP.	FMDADM = 99,43% eficaz

4.2. Achados

Reddy et al. (2020) concluíram que a utilização da Rede Bayesiana Dinâmica (DBN) juntamente ao meio de Mecanismo de Seleção de Funções com Lógica Nebulosa (MFSLnO) tiveram o desempenho mais eficaz se comparados com os modelos convencionais, por exemplo o meio MFSLnO padrão. Esta junção de processos de detecção de ataques foi considerada pelos autores como uma versão aprimorada da MFSLnO e pretendem, em estudos futuros, aplicá-lo às entregas de aplicativos de serviços pela internet, com o objetivo de que assim auxilie a computação em nuvem na detecção dos Ataques de Negação de Serviço Distribuído (DDoS).

No estudo de Elsayed et al. (2019) foi analisado as abordagens básicas no Aprendizado de Máquina (ML) devido à grande dificuldade em detectar os ataques, e, assim confirmaram que a Aprendizagem Profunda (DL) se tratava de uma importante ferramenta para extrair dados não rotulados e conseguir identificar ataques dentro dos Sistemas de Detecção de Intrusão (IDS). Já em 2022, no estudo de Wang et al., a fim de entender melhor sobre o ML, aplicaram a sua pesquisa diversas técnicas de Aprendizado de Máquina Supervisionado (SL), objetivando avaliar qual seria a melhor para detectar o DDoS. Dentre as técnicas utilizadas a “bagging tree” se destacou com uma precisão de 99,64% e em menor tempo do que as outras técnicas.

Sangodoyin et al. (2021) analisaram e classificaram os ataques DDoS utilizando as técnicas SL, em especial os meios Naive Bayes Gaussiano (GNB), Análise Discriminante Quadrática (QDA), K-Vizinhos Mais Próximos (k-NN) e Árvores de Decisão (CART), nos quais demonstraram uma enorme eficácia para detectar os ataques DDoS, porém a abordagem CART se mostrou mais estável se comparado aos outros métodos. Hamarshe et al. (2023), assim como nos estudos anteriores, utilizaram das técnicas de Aprendizado de Máquina e concluíram que o algoritmo Random Forest alcançou as expectativas com uma precisão de 68,9% para detectar ataques DDoS.

Para Tuan et al. (2020) aplicar o Aprendizado de Máquinas em Redes para suavizar os ataques DDoS demonstrou que mais de 98% do

tráfego de ataques pôde ser identificado e combatido. Já em 2021, o estudo de Tonkal et al. complementam a pesquisa e aprimoraram recursos do algoritmo NCA a fim de fazer com que os Aprendizado de Máquina melhorassem a eficácia para detectar os ataques, onde puderam concluir principalmente que a seleção das características dos ataques auxilia na classificação do mesmo. Dentre os meios utilizados pelos autores, o algoritmo Decision Tree teve uma precisão de 100% na verificação de ataques DDoS.

Em 2020, a pesquisa de Polat et al. analisou possíveis sistemas SDN para detectar ataques DDoS intervindo com os métodos do Aprendizado de Máquina. O estudo concluiu que foi satisfatório interligar os conteúdos pois grande parte dos dados teve desempenho superior a 80%, tanto na questão de detectar as navegações em rede ou nos ataques de softwares maliciosos para SDN.

Negera et al. (2022) abordaram, através de técnicas do Aprendizado de Máquina, sobre a detecção de ataques de Botnet em redes IoT habilitadas para SDN. A ameaça gerada por este tipo de ataque se demonstrou significativa, pois, dependendo da classificação do ataque, poderia facilmente ser exposto as vulnerabilidades dos dispositivos, evidenciando mais uma vez o potencial do Aprendizado de Máquina neste campo de atuação.

Khedr et al. (2023) em sua pesquisa, utilizaram meios diferentes dos estudos publicados anteriormente, tais como o framework FMDADM, no qual tem como objetivo prevenir os ataques DDoS, mesmo se tratar de um ataque com poucas chances de eficácia. Até o presente momento, esta estrutura superou as soluções de ponta em todos os termos da detecção, desde a taxa falsa até a especificidade ou precisão do ataque. Em 2022 Aslam et al. também haviam estudado sobre os framework’s para detectar ataques DDoS, no artigo publicado foi tratado sobre o framework AMLSDM, que se baseia em um modelo adaptativo do Aprendizado de Máquina para verificar os ataques em redes de tráfego habilitadas para SDN IoT, onde validaram sua eficácia de mitigação para classificação em tempo real.

5. Discussão

Os ataques de negação de serviço distribuído (DDoS) têm sido uma ameaça persistente à segurança cibernética, tornando-se mais sofisticados e difíceis de detectar com o passar dos anos. No entanto, a modernidade trouxe consigo ferramentas avançadas, como a inteligência artificial (IA), que revolucionaram a forma como enfrentamos essas ameaças.

A Inteligência Artificial é uma ferramenta poderosa que pode analisar grandes volumes de dados em tempo real, identificar padrões anômalos e tomar decisões rápidas. Isso a torna particularmente eficaz na detecção de ataques DDoS, que geralmente envolvem um grande número de solicitações maliciosas que sobrecarregam os servidores alvo.

A inteligência artificial tem sido uma poderosa aliada na detecção de ataques DDoS nos dias de hoje, proporcionando respostas rápidas e eficazes. No entanto, a modernidade da tecnologia impõe desafios constantes aos pesquisadores, que precisam se manter atualizados e adaptar suas abordagens para acompanhar a evolução das ameaças cibernéticas. À medida que a IA continua a desempenhar um papel fundamental na segurança cibernética, a colaboração entre pesquisadores e a inovação contínua serão essenciais para proteger as redes digitais em um mundo cada vez mais interconectado.

6. Conclusão

Contudo, com base nos estudos analisados, fica evidente que não existe um determinado método ou “melhor” meio para a detecção de ataques DDoS. A eficácia da detecção depende de diversos fatores, principalmente do tipo do ataque, o tipo da rede e os recursos disponíveis. Entretanto, é importante ressaltar a importância do Aprendizado de Máquina e das suas técnicas, tais como o Aprendizado de Máquinas Supervisionado, nas quais se mostram altamente promissores para detectar os ataques e em muitos casos saber lidar com dados não rotulados ou dos padrões complexos no tráfego. As redes e os frameworks também são utilizados nos dias de hoje como meio de detectar, avaliar, prevenir e mitigar os ataques DDoS.

Por tanto, a conclusão é de que a detecção eficaz nos ataques DDoS requer abordagem holística e

adaptativa. Organizações devem considerar as características específicas de suas redes e escolher técnicas e ferramentas promissoras para com suas necessidades, sendo crucial manter-se atualizado com o desenvolvimento da área de segurança cibernética para se manter adiante das ameaças que estão em constante evolução.

Referências:

Rodrigues, R. M., Fortuna, P., & Amaral, L. A. (2020). Distributed denial of service (DDoS) attacks and defense mechanisms: Classification, evolution and future directions. Computers & Security, 88, 101616.

Wang, L., Jia, R., Liu, S., Wang, H., Ren, K., & Lou, W. (2019). Harnessing the power of intelligence for mitigating DDoS attacks. IEEE Network, 33(5), 228-233.

Ludermir, Teresa Bernarda. Inteligência Artificial e Aprendizado de Máquina: estado atual e tendências. Estudos Avançados [online]. 2021, v. 35, n. 101 [Acessado 27 Setembro 2023], pp. 85-94.

Maidel De La Rosa Téllez, Mirelis Alcina Reyes, and Ariel Céspedez Pérez. "Estrategia Cognitiva Para Impedir Ataques Ddos En Servidores Web." Opuntia Brava 13.1 (2021): 102-12. Web.

Karel Rodríguez Carmenates, Reisel González Pérez, and Pedro Manuel Puig Díaz. "Implementación De Servidores Seguros Contra Ataques DDOS." Serie Científica De La Universidad De Las Ciencias Informáticas 10.6 (2019): Serie Científica De La Universidad De Las Ciencias Informáticas, 2019, Vol.10 (6). Web.

HAMARSHE, Ahmad; ASHQAR, Huthaifa I.; HAMARSHEH, Mohammad. Detection of DDoS Attacks in Software Defined Networking Using Machine Learning Models. In: **International Conference on Advances in Computing Research**. Cham: Springer Nature Switzerland, 2023. p. 640-651.

W. I. Khedr, A. E. Gouda and E. R. Mohamed, "FMDADM: A Multi-Layer DDoS Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks,"

in IEEE Access, vol. 11, pp. 28934-28954, 2023.

Tuan NN, Hung PH, Nghia ND, Tho NV, Phan TV, Thanh NH. A DDoS Attack Mitigation Scheme in ISP Networks Using Machine Learning Based on SDN. *Electronics*. 2020; 9(3):413.

POLAT, Huseyin; POLAT, Onur; CETIN, Aydin. Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models. **Sustainability**, v. 12, n. 3, p. 1035, 2020.

TONKAL, Özgür et al. Machine learning approach equipped with neighbourhood component analysis for DDoS attack detection in software-defined networking. **Electronics**, v. 10, n. 11, p. 1227, 2021.

NEGERA, Worku Gachena et al. Review of botnet attack detection in SDN-enabled IoT Using machine learning. **Sensors**, v. 22, n. 24, p. 9837, 2022.

WANG, Song et al. Detecting flooding DDoS attacks in software defined networks using supervised learning techniques. **Engineering Science and Technology, an International Journal**, v. 35, p. 101176, 2022.

SANGODOYIN, Abimbola O. et al. Detection and classification of ddos flooding attacks on software-defined networks: A case study for the application of machine learning. **IEEE Access**, v. 9, p. 122495-122508, 2021.

ASLAM, Muhammad et al. Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for SDN-enabled IoT. **Sensors**, v. 22, n. 7, p. 2697, 2022.

ELSAYED, Mahmoud Said et al. Machine-learning techniques for detecting attacks in SDN. In: **2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT)**. IEEE, 2019. p. 277-281.

REVATHI, M.; RAMALINGAM, V. V.; AMUTHA, B. A machine learning based detection and mitigation of the DDOS attack by using SDN controller framework. **Wireless Personal Communications**, p. 1-25, 2021.