Ataques DoS e DDoS em IoT: Classificação, Impacto e Técnicas de Detecção

Diana Laura Fernández Duarte (INATEL)[1], Alfredo Jesús Arbolaez Fundora (INATEL)[2]
diana.duarte@mtel.inatel.br[1], alfredo.fundora@mtel.inatel.br[2]

***Resumo*—A crescente popularidade da Internet das Coisas (IoT) nos últimos anos abre novas oportunidades em um mundo em que diversos dispositivos se conectam e interagem entre si por meio da Internet para automatizar uma infinidade de tarefas. Junto com essas oportunidades, surgem novos desafios de segurança como resultado da heterogeneidade e dos recursos limitados que caracterizam esses dispositivos inteligentes. Essas vulnerabilidades os expõem a ataques cibernéticos, mais comumente ataques de negação de serviço (DoS) e de negação de serviço distribuída (DDoS). Este artigo faz uma análise dos diferentes ataques de DoS e DDoS que uma rede de IoT pode sofrer em cada uma das camadas de sua arquitetura, além de compilar algumas das técnicas propostas na literatura para a detecção desses ataques, desde as tradicionais até métodos mais avançados que incluem algoritmos de aprendizado de máquina (ML) e aprendizado profundo (DL).**

I. Introdução

A crescente adoção da IoT, impulsionada por seu imenso potencial de otimização de todos os tipos de tarefas, desde as mais simples em casa até as mais complexas em setores como agricultura, indústria e saúde, torna esse ecossistema um alvo extremamente atraente para criminosos cibernéticos e hackers. A interconexão maciça desses dispositivos gera um enorme volume de dados que precisam ser processados, filtrados, transferidos e armazenados, com um alto grau de complexidade em termos de segurança, comprometendo os princípios dos sistemas de IoT focados em escalabilidade, facilidade de uso e interoperabilidade.

Os baixos requisitos de energia desses dispositivos de IoT, bem como sua capacidade limitada de armazenamento e processamento, fazem com que eles dependam da computação em nuvem ou de borda para processamento adicional. Seu alto grau de heterogeneidade, o uso de protocolos de comunicação de baixo consumo de energia e baixa largura de banda e a exposição a diferentes condições ambientais são apenas algumas das características que tornam os métodos padrão de prevenção e mitigação de ameaças ineficientes nessas redes.

A segurança e a privacidade do usuário foram comprometidas em várias ocasiões devido à falta de atenção dos fabricantes à segurança dos dispositivos. Os ataques comumente usados incluem ataques DoS e DDoS, que são o foco da pesquisa deste projeto. Eles tendem a ser mais frequentes do que outros tipos de ataques devido à sua simplicidade em termos de conhecimento e ferramentas de software necessárias. Seu objetivo é impedir que um dispositivo específico de IoT ou uma rede inteira forneça um determinado serviço, o que leva ao desencadeamento de vários problemas críticos, principalmente em cenários que envolvem troca de informações em tempo real [1].

Com base em uma análise da literatura disponível, a Seção II deste projeto descreve como esses ataques podem ser implementados, enquanto a Seção III discute alguns dos métodos propostos por diferentes autores para sua detecção. Por fim, a Seção IV apresenta as conclusões obtidas durante a pesquisa.

II. Ataques DoS e DDoS em ambientes IoT

Um ataque de DoS consiste em sobrecarregar a vítima com uma quantidade excessiva de solicitações de serviço, saturando-a com um alto tráfego de dados, o que resulta em uma congestão deliberada na rede, interrompendo o serviço para os usuários legítimos. O ataque de DDoS é uma variante mais complexa do DoS, na qual o atacante utiliza múltiplas fontes simultaneamente para sobrecarregar o alvo. Essas fontes, em sua maioria, são dispositivos inteligentes comprometidos e controlados remotamente por uma entidade maliciosa utilizando um Servidor de Comando e Controle (CCS), que frequentemente é outro dispositivo comprometido. Os dispositivos comprometidos formam uma botnet, uma rede de dispositivos controlados remotamente pelo atacante. Esses ataques não são exclusivos das aplicações IoT, alguns são herdados diretamente das redes clássicas, enquanto outros têm como alvo explorar uma fraqueza própria dos objetos inteligentes, como a sua capacidade limitada de bateria. [2]

A seguir, são descritos os ataques DoS mais comuns nas diferentes camadas da arquitetura IoT.

A. Ataques à Camada de Percepção

A camada de percepção é composta por sensores que coletam informações do ambiente e atuadores que executam determinadas ações em correspondência com os dados obtidos. Os sensores, também conhecidos como nós, são suscetíveis a vários ataques que buscam impedi-los de cumprir sua função de coleta de dados, dificultando a transferência de informações para as camadas superiores [3]. Os ataques comuns incluem os seguintes:

- Ataques de interferência: O objetivo desses ataques é inundar as ondas de rádio com ruído de frequência, o que pode ser particularmente prejudicial, pois a maioria dos dispositivos inteligentes se comunica sem fio. O invasor pode emitir o sinal de interferência de três maneiras diferentes: constantemente, somente quando detecta uma transmissão no meio ou aleatoriamente [1].

- Ataques de drenagem de bateria: Esses ataques visam drenar a bateria de dispositivos projetados para consumir pouca energia e operar com bateria por longos períodos. Eles usam técnicas como a prevenção do sono ou a inundação do dispositivo com solicitações de serviço desnecessárias que, consequentemente, levam ao seu desligamento [1].
- Ataques de desconexão: Os ataques de desconexão visam interromper a conexão entre os dispositivos de IoT e a rede ou a Internet. Eles são executados por invasores que obtêm acesso não autorizado ao canal de comunicação e interrompem a transferência de pacotes de dados [1].
- Ataques de dessincronização: Esses ataques consistem no envio de sinais de tempo falsos ou na manipulação deliberada das informações de tempo na rede para interromper o sincronismo existente entre os diferentes dispositivos em uma rede de IoT, sincronismo esse que possibilita a coordenação de ações e a troca eficiente de informações [1].

B. Ataques à Camada de Rede

A camada de rede é responsável por enviar informações da camada de percepção para a unidade de computação para processamento posterior. Nessa camada, os invasores tentam enfraquecer os protocolos de roteamento para interromper a transferência de dados [3]. A seguir estão os tipos mais comuns de ataques de DoS nessa camada.

- Ataques de descarte de pacotes: Nós mal-intencionados descartam intencionalmente um conjunto de pacotes ou até mesmo todos os pacotes que deveriam ser encaminhados ao seu destino. Uma variante desse ataque é o encaminhamento seletivo, no qual o invasor encaminha seletivamente alguns pacotes e descarta outros. Uma forma mais extrema desse ataque é o chamado Black Hole, em que o nó comprometido descarta todos os pacotes que recebe, bloqueando completamente o fluxo de dados para o seu destino. Outra alternativa usada pelos invasores é a personificação de um nó vizinho legítimo para interceptar e manipular a troca de informações entre dispositivos, afetando protocolos de roteamento como o Protocolo de Roteamento para Redes de Baixa Potência e com Perdas (RPL) [1].
- Ataques de inundação: Consistem em inundar a rede com uma quantidade excessiva de dados e solicitações até o ponto de sobrecarga. Por exemplo, um ataque de inundação de TCP consiste em enviar um grande número de pacotes SYN ao dispositivo de destino para, eventualmente, não concluir o processo de handshake e deixar o dispositivo de destino esperando e sobrecarregado pelo número de conexões incompletas. Outra variante desses ataques consiste no envio de um grande número de pacotes de dados com o objetivo de consumir toda a largura de banda disponível do link de rede ou no envio de pacotes fragmentados a um determinado dispositivo para transbordar seu buffer. Os ataques DDoS de baixa taxa buscam gerar um baixo volume de tráfego malicioso, abaixo do limite de detecção das técnicas de atenuação de DDoS, permitindo que o sistema seja gradualmente sobrecarregado sem ser detectado [1].
- Ataques enganosos de redirecionamento de tráfego: Os nós mal-intencionados procuram redirecionar o tráfego para si mesmos clonando a identidade de outros nós, usando várias identidades falsas ou manipulando a seleção de rota ideal por outros nós. Eles fazem isso enviando mensagens com um número de versão de rede maior do que o real, enviando mensagens falsas para indicar que têm uma rota melhor para um determinado destino, alterando sua classificação para se colocarem em uma posição estratégica na hierarquia de roteamento ou escolhendo uma rota ineficiente para retardar o fornecimento de seus dados pela rede [1].
- Ataques adversários contra o aprendizado de máquina: Envolvem a manipulação dos dados que o modelo de aprendizado de máquina usa para se treinar, permitindo que o invasor entre no sistema sem ser detectado [1].

C. Ataques à Camada de Aplicativos

Os ataques nesse nível são semelhantes aos ataques identificados na camada de inundação, só que eles atacam protocolos específicos da camada de aplicativos, como MQTT, CoAP e HTTP, com o objetivo de impedir que os dispositivos inteligentes forneçam seus serviços ao usuário final. Os tipos mais comuns de ataques DDoS incluem inundação HTTP, ataque Slowloris, inundação GET/POST e ataques a diferentes servidores vulneráveis [4].

III. Medidas para mitigar ataques DoS e DDoS em ambientes IoT

Existem algoritmos clássicos para a detecção de ataques DoS e DDoS, principalmente com base na análise de tráfego. Seu objetivo é detectar padrões ou anomalias que possibilitem a identificação de um ataque em andamento. Diferentes técnicas são usadas para estimar esses padrões, algumas das quais estão listadas abaixo.

- Cálculo de parâmetros de confiança para determinar se um nó pode ser considerado seguro ou mal-intencionado, com base na comparação com determinados valores de limite predefinidos. Um valor de confiança alto indica que o algoritmo está muito confiante de que o comportamento incomum do tráfego se deve a um ataque, enquanto um valor mais baixo sugere que o comportamento pode ser devido a outros fatores [1].
  Alguns autores propõem o uso da Função de Distribuição de Probabilidade Beta (BPDF) para prever o nível de segurança de um nó com base em seu comportamento. Essa função permite modelar a confiança com base em dados dinâmicos e atualizáveis, com mais precisão do que os métodos baseados em limites fixos [1]. Outras pesquisas propõem usar o método de máxima verossimilhança para calcular a probabilidade de que o comportamento observado no sistema seja resultado de

um ataque, com base na suposição de que os dados coletados seguem uma distribuição de probabilidade conhecida. Ao comparar o comportamento real com o valor esperado para essa distribuição, é possível determinar se o sistema está sendo atacado ou se está operando normalmente. Em [5], propõem uma técnica de detecção de intrusão que faz uso do método de máxima verossimilhança para calcular os parâmetros da função beta probabilística que estima o grau de conformidade de um nó.

Outras abordagens consideram a influência de diferentes fontes, como sistemas de detecção de intrusão, logs de rede e análise do comportamento do usuário, para medir a confiabilidade do sistema. Cada uma dessas fontes é representada por uma função de crença. Elas são combinadas usando uma fórmula matemática para calcular o grau geral de crença no sistema. É uma técnica complexa que exige a coleta de informações sobre várias fontes de evidência para obter um valor preciso para o nível de confiança [1].

Outra técnica proposta na literatura é o teste de Kolmogorov-Smirnov. Esse teste consiste em comparar a função de distribuição cumulativa (CDF) da saída do algoritmo com a CDF de uma distribuição de referência, a fim de medir o nível de confiança do nó. Em [6], eles usam o teste Kolmogorov-Smirnov como parte de seu sistema de autenticação baseada em confiança.

- Métodos baseados na verificação de autenticação e identificação para complementar os algoritmos de detecção. Algumas abordagens consideram a geração de um token criptográfico para verificar e autenticar os nós da rede, outras propõem a geração de respostas exclusivas para autenticar cada dispositivo de IoT com base nas propriedades físicas exclusivas dos circuitos integrados, enquanto outras pesquisas propõem o uso do Chip de Módulo de Plataforma Confiável (TPM) para a geração desse identificador único. O autor de [7] propõe o uso desse chip para gerenciar e armazenar chaves criptográficas com segurança, reduzindo a carga de processamento dos nós de IoT.

  Alguns autores consideraram o uso da tecnologia blockchain para estabelecer um registro distribuído de todos os dispositivos de IoT em uma rede, de modo que as transações sejam armazenadas de forma transparente e anomalias no comportamento do tráfego devido a ataques de DoS sejam detectadas. Algumas pesquisas propõem o uso de contratos inteligentes da Ethereum para evitar ataques de DoS [4].

  O uso de filtros Bloom, estruturas de dados probabilísticos que identificam se um elemento é membro de um conjunto, é outra técnica proposta, embora tenha limitações, pois esses filtros não são capazes de fornecer informações detalhadas sobre o ataque ou sua origem. Em [8], eles propõem um esquema de filtro Bloom aprimorado que melhora a eficiência da memória e reduz o tempo de processamento da pesquisa para detecção de intrusão na IoT. Em [9], eles implementam um mecanismo leve chamado BLAM para resolver ataques de inundação de interesse (IFA). Cada nó da IoT é equipado com um filtro Bloom para detectar comportamentos suspeitos. Esse esquema reduz o consumo de memória e melhora a latência, mas tem uma pequena perda de precisão.
- Análise de rede para identificar anomalias, como picos de tráfego, várias solicitações de um único ponto e pacotes malformados ou com cabeçalhos incorretos. Essa abordagem enfrenta limitações devido à heterogeneidade dos dispositivos e à falta de padronização nos sistemas de IoT, o que dificulta a implementação de soluções uniformes e gera altos custos de armazenamento e processamento.

  Os algoritmos baseados em regras definem limites específicos para analisar o comportamento da rede usando ferramentas como IDS, firewalls e análise de tráfego. No entanto, eles exigem atualizações manuais, o que é ineficiente em termos de escalabilidade e tempo. Por outro lado, os algoritmos baseados em perfis pré-criam um perfil para cada nó de IoT, que é comparado com o comportamento atual para detectar anomalias, como consumo excessivo de recursos ou picos de tráfego, que podem indicar ataques de DoS, mas também apresentam desafios em ambientes dinâmicos. Outra abordagem é o estabelecimento de especificações formais ou semiformais usando modelos matemáticos que definem o comportamento esperado de diferentes componentes do sistema e possíveis fontes de ataques. Diferentes algoritmos estatísticos também são usados para estabelecer limites para detectar comportamentos anômalos no tráfego da rede. Isso exige a coleta de um grande volume de dados, o que pode ser complexo devido à capacidade limitada de processamento dos dispositivos de IoT. Os dados coletados podem conter informações confidenciais, o que gera preocupações significativas com a privacidade [1].

As técnicas descritas acima são ineficientes diante de ataques complexos porque classificam o tráfego de rede atual como normal ou mal-intencionado com base em uma comparação com determinadas regras ou padrões predefinidos. As soluções baseadas em inteligência artificial, como os algoritmos de aprendizado de máquina (ML) e aprendizado profundo (DL), são mais confiáveis e eficazes, permitindo que aprendam padrões específicos de ataques de DoS/DDoS em redes de IoT [10]. Os algoritmos mais comumente usados para soluções baseadas em ML e DL estão listados abaixo.

- Técnicas clássicas de ML supervisionado, que incluem diferentes algoritmos, como Árvore de Decisão, Random Forest, Máquina de Vetor de Suporte, Classificadores Naive Bayes e K-Nearest Neighbor.

  A árvore de decisão é uma técnica usada para resolver problemas de regressão e classificação. Sua estrutura de árvore é composta de nós internos que representam recursos do conjunto de dados, ramos que representam regras de decisão e nós de folhas que representam os resultados. Para determinar a classe à qual um determinado dado do conjunto de dados pertence, o algoritmo

compara os valores do nó raiz com o valor correspondente no conjunto de dados. Com base nessa comparação, ele seleciona uma ramificação e repete o processo em nós internos sucessivos até chegar ao nó folha, que representa a classe prevista. O algoritmo Random Forest usa um grande número de árvores de decisão individuais. Cada árvore prevê uma classe, e a classe que se repete o maior número de vezes é a previsão do modelo [10].

O algoritmo Naive Bayes é um algoritmo de classificação probabilística simples que usa probabilidades condicionais para determinar se um recurso pertence ou não a uma determinada classe. Os recursos mais importantes são selecionados, enquanto os menos relevantes são eliminados, de modo que o sistema se torna mais leve. Isso não deve afetar o nível de precisão do classificador. O algoritmo K-Nearest Neighbors é um método de aprendizado supervisionado, valioso para resolver problemas de classificação. Para prever a classe à qual uma amostra pertence, ele identifica a classe mais repetida entre as k amostras mais próximas no conjunto de dados de treinamento. Esse valor de k é um fator crítico para a precisão do modelo [10].

Os autores de [11] propõem um novo sistema de detecção de intrusos para prevenir ataques DoS em ambientes IoT baseados em redes centradas na informação (ICN). O sistema combina os algoritmos Máquinas de Vetores de Suporte, Random Forest e K-Nearest Neighbors, e é baseado na arquitetura NDN, utilizando o simulador ndnSIM. Em [12], propõem um sistema de detecção sequencial de ataques de botnet híbrido que combina Redes Neurais Artificiais, o algoritmo J48 para a construção de árvores de decisão, e Naive Bayes.

- Técnicas de DL supervisionado, que comumente utilizam modelos avançados, como Redes Neurais Profundas (DNN), Redes de Crenças Profundas (DBN), Redes Neurais Feedforward (FNN), Redes Neurais Recorrentes (RNN) e Redes Neurais Convolucionais (CNN).

  As DNNs imitam a estrutura e a função do cérebro humano, com camadas ocultas entre as camadas de entrada e saída, permitindo à rede aprender representações complexas a partir dos dados fornecidos. No artigo [13], faz-se uso de DNNs para melhorar a precisão e a eficiência dos Sistemas de Detecção de Intrusões em Redes (NIDS).

  As DBNs são um tipo de rede neural profunda composta por várias camadas de neurônios conectados entre si, mas sem conexões dentro de cada camada. No artigo [14], propõe-se o uso de um módulo de DBN combinado com técnicas de balanceamento de classes para evitar o desequilíbrio nos conjuntos de dados, enfrentando as ameaças cibernéticas mais frequentes.

  As FNNs se diferenciam das redes neurais recorrentes porque a informação se move em uma única direção, sem formar ciclos ou laços. No artigo [15], é proposto um modelo de detecção de intrusos baseado em FNN, com resultados de precisão de 99%. Esse modelo foi comparado com outros classificadores, como o Autoencoder, superando-os em termos de eficiência e precisão na detecção de ataques.

  As RNNs são um tipo de rede neural artificial projetada para o processamento de dados sequenciais, com capacidade de memória para reter informações de entradas anteriores, o que as diferencia das FNNs. No artigo [16], é proposta uma nova técnica para o monitoramento do tráfego em redes IoT, integrando um módulo de Memória de Longo e Curto Prazo (LSTM). A LSTM é um tipo especial de RNN com capacidade para aprender e lembrar informações por períodos prolongados. Essa técnica demonstrou alta capacidade para detectar ataques em diferentes momentos, até mesmo desde o início de um ataque.

  Uma CNN é um tipo de rede neural artificial inspirada no comportamento da córtex visual primária do cérebro humano, sendo ideal para o processamento e análise de imagens. Os autores de [17] propõem uma metodologia que converte dados de tráfego de rede em imagens, utilizando CNNs. Essa metodologia alcançou uma precisão de 99,99% na detecção de ataques.

IV. Conclusões

As grandes violações de segurança resultantes do uso maciço de dispositivos de IoT nos últimos anos são o foco da atenção de vários pesquisadores que buscam atenuá-las por meio de técnicas criativas e robustas. Para a detecção de ataques de DoS e DDoS especificamente, vários autores propõem métodos baseados no cálculo de parâmetros de confiança, detecção de intrusão ou análise de rede, com base em determinados valores de limite predefinidos. Embora essas técnicas tradicionais sejam ineficientes diante de ataques complexos, os métodos baseados em aprendizado profundo e automático que memorizam diferentes padrões de ataques específicos são soluções mais completas e eficazes para a identificação de anomalias e a prevenção de tais ataques.

References

[1] M. R. Kadri, A. Abdelli, J. Ben Othman, and L. Mokdad, "Survey and classification of dos and ddos attack detection and validation approaches for iot environments," *Internet of Things*, vol. 25, p. 101021, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S254266052300344X

[2] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[3] N. Mishra and S. Pandya, "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review," *IEEE Access*, vol. 9, pp. 59 353–59 377, 2021.

[4] D. M. Rajan and S. Sathya Priya, "Ddos mitigation techniques in iot: A survey," in *2022 International Conference on IoT and Blockchain Technology (ICIBT)*, 2022, pp. 1–7.

[5] M. Surendar and A. Umamakeswari, "Indres: An intrusion detection and response system for internet of things with 6lowpan," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2016, pp. 1903–1908.

[6] Y. Durasiamy, S. Priya, M. Braveen, S. Krishnan, S. Nachiyappan, A. Mehbodniya, M. U. A. Ayoobkhan, and M. Sivaram, "Novel dos attack detection based on trust mode authentication for iot," *Intelligent Automation Soft Computing*, vol. 34, pp. 1505–1522, 01 2022.

[7] F. Medjek, D. Tandjaoui, I. Romdhani, and N. Djedjig, "A trust-based intrusion detection system for mobile rpl based networks," in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2017, pp. 735–742.

[8] F. Gebretsadik, S. Nayak, and R. Patgiri, "ebf: an enhanced bloom filter for intrusion detection in iot," *Journal of Big Data*, vol. 10, 06 2023.

[9] G. Liu, W. Quan, N. Cheng, B. Feng, H. Zhang, and X. S. Shen, "Blam: Lightweight bloom-filter based ddos mitigation for information-centric iot," in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–7.

[10] A. Ashraf and W. M. Elmedany, "Iot ddos attacks detection using machine learning techniques: A review," in *2021 International Conference on Data Analytics for Business and Industry (ICDABI)*, 2021, pp. 178–185.

[11] R. Bukhowah, A. Aljughaiman, and M. M. H. Rahman, "Detection of dos attacks for iot in information-centric networks using machine learning: Opportunities, challenges, and future research directions," *Electronics*, vol. 13, no. 6, 2024. [Online]. Available: https://www.mdpi.com/2079-9292/13/6/1031

[12] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Machine learning-based iot-botnet attack detection with sequential architecture," *Sensors*, vol. 20, no. 16, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/16/4372

[13] H. Qiu, T. Dong, T. Zhang, J. Lu, G. Memmi, and M. Qiu, "Adversarial attacks against network intrusion detection in iot systems," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10 327–10 335, 2021.

[14] W. F. Elsersy, M. Samy, and A. ElShamy, "Network intrusion detection using deep belief network (dbn)," in *2024 Intelligent Methods, Systems, and Applications (IMSA)*, 2024, pp. 193–198.

[15] P. Kalpana, P. Srilatha, G. S. Krishna, A. Alkhayyat, and D. Mazumder, "Denial of service (dos) attack detection using feed forward neural network in cloud environment," in *2024 International Conference on Data Science and Network Security (ICDSNS)*, 2024, pp. 1–4.

[16] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K.-K. R. Choo, and R. M. Parizi, "An ensemble of deep recurrent neural networks for detecting iot cyber attacks using network traffic," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8852–8859, 2020.

[17] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, "Iot dos and ddos attack detection using resnet," in *2020 IEEE 23rd International Multitopic Conference (INMIC)*, 2020, pp. 1–6.