Mapeamento Sistemático de Ataques e Mecanismos de Defesa em Redes IPv4 e IPv6

Paulemir S. Soares, Demilly F. Ferreira da Silva, Luciana P. Oliveira (IFPB, Campus João Pessoa)

E-mails: paulemir.sousa@academico.ifpb.edu.br, demilly.silva@ifpb.edu.br, luciana.oliveira@iesp.edu.br .

Área de conhecimento: 1.03.00.00-7 Ciência da Computação.

Palavras-chave: segurança de redes; ataques DDoS; IPv4; IPv6; detecção de ataques; mitigação de ataques.

1. Introdução

A crescente dependência de serviços baseados na Internet expõe redes e sistemas a uma variedade de ameaças, tornando a segurança de rede uma necessidade fundamental. Estudos recentes, como Camargo et al. (2024), mostram que a escassez de endereços IPv4 impõe desafios ao monitoramento, mas pode ser contornada com amostragem inteligente. A transição e coexistência das redes IPv4 e IPv6 introduzem novas complexidades e vetores de ataque, exigindo abordagens de segurança adaptadas a ambos os protocolos. Ataques de inundação (flooding), como os direcionados ao ICMPv6, exploram vulnerabilidades específicas do novo protocolo (Elejla et al., 2022), enquanto técnicas como spoofing de IP continuam a ser um desafio tanto em IPv4 quanto em IPv6, mascarando a origem dos ataques e dificultando a identificação dos atacantes (Gomathi & Karthikeyan, 2015).

Este trabalho apresenta um levantamento de diferentes tipos de ataques de segurança, com foco em DDoS e flooding, em ambientes IPv4 e IPv6, e discute mecanismos de detecção e mitigação propostos na literatura. Desta forma este estudo busca responder às seguintes perguntas:

1. Quais são as principais diferenças entre as vulnerabilidades dos protocolos IPv4 e IPv6?
2. Quais técnicas têm se mostrado mais eficazes na mitigação de ataques DDoS em ambientes IPv4 e IPv6?
3. De que maneira as arquiteturas baseadas em SDN e algoritmos de aprendizado de máquina contribuem para a segurança em redes IP?

2. Materiais e Métodos

Este estudo fundamenta-se em uma revisão bibliográfica sistemática com foco na análise de ataques à segurança de redes e seus respectivos mecanismos de defesa, considerando ambientes IPv4 e IPv6. A metodologia foi dividida em duas etapas: Fase de Planejamento e Fase de Execução.

2.1 Fase de Planejamento

Nesta fase, foram definidos os critérios de inclusão(CI) e exclusão(CE) dos artigos coletados. Como critérios de exclusão(CE), foram excluídos: publicações com acesso restrito; e materiais como livros e artigos que não caracterizem estudos comparativos envolvendo IPv4 e IPv6 no âmbito de ataques cibernéticos. Os critérios de inclusão(CI) foram: estudos que contenham informações para responder às perguntas descritas na Seção 1.

Foi escolhida a string de busca ("IPv4" AND "IPv6" AND "cyber attack" AND "comparison") por sua relação com o estudo proposto, e foram selecionadas as seguintes bases de dados: ResearchGate(22), ScienceDirect(58), Google Scholar (385) e IEEE Xplore (1).

2.2 Fase de Execução

A string de busca foi aplicada nas bases mencionadas, resultando na coleta inicial de 466 artigos. A triagem ocorreu em três etapas: descarte de artigos com acesso restrito ou sem liberação dos autores; exclusão de estudos não comparativos sobre IPv4/IPv6; e análise final de 150 artigos, dos quais 32 foram pertinentes e 9 selecionados. Esses estudos abrangem publicações desde as primeiras comparações de vulnerabilidades até trabalhos recentes

(31/03/2025). Os artigos encontram disponíveis no Github[1].

3. Resultados e discussão

Os resultados apresentados a seguir correspondem às respostas obtidas para os questionamentos formulados na etapa introdutória deste estudo, evidenciando a efetividade, limitações e especificidades de cada abordagem no contexto analisado.

3.1 Quais são as principais diferenças entre as vulnerabilidades dos protocolos IPv4 e IPv6?

A análise comparativa mostra que o IPv6, apesar de introduzir avanços como suporte nativo ao IPsec e autoconfiguração de endereços (SLAAC), também apresenta novos vetores de ataque. A obrigatoriedade do ICMPv6, por exemplo, amplia a superfície de ataque em relação ao IPv4, onde o ICMP pode ser filtrado com mais liberdade. Além disso, o IPv6 ainda sofre com vulnerabilidades conhecidas, como o spoofing de IP, principalmente em ambientes de transição e redes híbridas. Em contextos industriais, a coexistência do IPv4 e IPv6 com protocolos legados como PROFIBUS e MODBUS acentua esses desafios, exigindo modelos matemáticos dinâmicos e mecanismos automatizados de resposta, conforme demonstrado por Moulika & Palanisamy (2024).

3.2 Quais técnicas têm se mostrado mais eficazes na mitigação de ataques DDoS em ambientes IPv4 e IPv6?

O estudo identificou abordagens como o uso de deep learning para detecção de tráfego anômalo (Elejla et al., 2022), além de mecanismos de filtragem e traceback já consolidados no IPv4 e adaptados para o IPv6. Destacam-se as arquiteturas que operam na borda da rede, como a proposta de Pimpalkar & Patil (2015), e as soluções voltadas para ICMPv6 flooding, como as de Ashimi & Adeniji (2020), que aproveitam a visibilidade centralizada do paradigma SDN para mitigar ataques de forma eficaz. Além disso, Camargo et al. (2024) demonstraram que técnicas de amostragem inteligente em telescópios de rede reduzidos permitem manter alta eficácia na detecção de ataques, mesmo diante da escassez de endereços IPv4 - um resultado essencial para organizações que enfrentam restrições de recursos de monitoramento. A tabela a seguir compila as técnicas de detecção/mitigação em IPv4 e IPv6.

Tabela 1 – Análise comparativa entre critérios associados à vulnerabilidades entre os protocolos IPv4 e IPv6.

Técnica	IPv4	IPv6	Fonte
Orquestração com Ansible para ataques simulados (SYN, HTTP, SMTP)	Simula ataques em rede real com sucesso; permite avaliação de desempenho e defesa	Mesma eficácia geral, mas com diferenças nos impactos medidos entre IPv4 e IPv6	Čerňanský, Huraj & Šimon (2020)
Combinação de filtragem e rastreamento de pacotes (Packet Filtering + Tracing)	Utiliza ingress/egress filtering e tracing; eficiente contra IP spoofing em IPv4	Aplicável, mas mais difícil rastrear origem por causa da estrutura do IPv6	Gomathi & Karthikeyan (2015)
Filtragem com verificação criptográfica de IPs spoofados	Classificação e bloqueio de pacotes em roteadores de borda com bons resultados	Aplicável, mas exige adaptações para cabeçalhos e autenticação ICMPv6	Pimpalkar & Patil (2015)
Mitigação de ataques DDoS em redes SDN habilitadas para IPv6	SDN aplicado em IPv4 em poucos estudos	SDN integrada com IPv6 permite resposta coordenada e mitigação eficaz	Ashimi & Adeniji (2020)
Detecção de ataques ICMPv6 com Deep Learning (LSTM)	Não aplicável – ataque ICMPv6 não existe no IPv4	Altamente eficaz; detecção com acurácia >98% usando LSTM e seleção de atributos	Elejla et al. (2022)
Modelo Matemático dinâmico para MES	Integra protocolos industriais com monitoramento IP	Mesmo framework, com suporte a IPv4 e IPv6	Moulika & Palanisamy(2024)

3.3 De que maneira as arquiteturas baseadas em SDN e algoritmos de aprendizado de máquina contribuem para a segurança em redes IP?

As soluções baseadas em machine learning têm se mostrado promissoras, especialmente na detecção de padrões de tráfego malicioso em tempo real (Mohay et al., 2011). A combinação com SDN permite uma resposta

[1]<https://github.com/mestradords20251/mestrado.git>

mais ágil e adaptativa aos ataques, aproveitando a flexibilidade e programabilidade da rede. O uso de redes neurais convolucionais e recorrentes, por exemplo, tem se destacado na detecção de ataques específicos ao IPv6, como os baseados em ICMPv6.

A síntese crítica das abordagens permitiu identificar padrões metodológicos, práticas recorrentes e desafios técnicos. Ademais, possibilitou o mapeamento de tendências no desenvolvimento de soluções robustas, escaláveis e resilientes para a proteção de redes operando sob os protocolos IPv4 e IPv6, frente ao aumento das ameaças cibernéticas. A combinação de técnicas tradicionais (filtragem, traceback) com abordagens modernas (machine learning, SDN) representa o caminho mais eficaz para a mitigação de ameaças em ambientes heterogêneos.

5. Considerações finais

Este trabalho realizou um levantamento de ataques de segurança, com ênfase em DDoS e flooding, em redes IPv4 e IPv6, analisando diferentes mecanismos de detecção e mitigação propostos na literatura. Os estudos de Pimpalkar & Patil (2015), Cernansky et al. (2020), Mohay et al. (2011), Gomathi & Karthikeyan (2015), Ashimi & Adeniji (2020), Elejla et al. (2022), além de trabalhos mais recentes como Camargo et al. (2024), Al-Azzawi & Lencse (2024) e Moulika & Palanisamy (2024), ilustram a complexidade do problema e a diversidade de soluções, incluindo abordagens voltadas à escassez de endereços IPv4, tecnologias de transição e ambientes industriais IoT. As soluções variam de técnicas criptográficas e de filtragem a métodos baseados em machine learning e SDN. Conclui-se que a segurança em redes IP é um campo dinâmico, onde a combinação de estratégias e a adaptação constante às novas tecnologias como o IPv6, são essenciais para mitigar ameaças.

Referências

AL-AZZAWI, A.; LENCSE, G. Methodology for the security analysis of IPv4-as-a-Service IPv6 transition technologies. Computer Journal, 2024. DOI:https://doi.org/10.1093/comjnl/bxae123.

ASHIMI, Q. O.; ADENIJI, O. D. Detection and mitigation of flood attacks in IPv6 enabled software defined networks. **Advances in Research**, v. 21, n. 8, p. 1-14, 2020. DOI: https://doi.org/10.9734/air/2020/v21i830221.

CAMARGO, A. V. C.; BERTHOLDO, L. M.; GRANVILLE, L. Z. Less is More? Exploring the Impact of Scaled-Down Network Telescopes on Security andResearch. IEEE Access, v. 12, p. 29854-29871, 2024. DOI: https://doi.org/10.1109/ACCESS.2024.3367842.

CERNANSKY, M.; KOTESKA, B.; JOLOUDEH, H. Controlled DDoS attack on IPv4/IPv6 network using distributed computing infrastructure. **Journal of Information and Organizational Sciences**, v. 44, n. 2, p. 291-305, 2020. DOI: https://doi.org/10.31341/jios.44.2.6.

ELEJLA, O. E.; ANBAR, M.; HAMOUDA, S.; FAISAL, S.; BAHASHWAN, A. A.; HASBULLAH, I. H. **Deep-Learning-Based Approach to Detect ICMPv6 Flooding DDoS Attacks on IPv6 Networks.** *Applied Sciences*, [S. l.], v. 12, n. 12, p. 6150, 16 jun. 2022. DOI: https://doi.org/10.3390/app12126150.

PIMPALKAR, A. S.; BHAGAT PATIL, A. R. Defense against DDoS attacks using IP address spoofing. **International Journal of Innovative Research in Computer and Communication Engineering**, v. 3, n. 3, p. 2251-2256, 2015.

GOMATHI, S.; KARTHIKEYAN, E. A new approach to detect, filter and trace the DDoS attack. In: UGC SPONSORED NATIONAL CONFERENCE ON ADVANCED NETWORKING AND APPLICATIONS, 2015, Udumalpet. **Anais** [...]. Udumalpet: [s.n.], 2015.

MOHAY, George; AHMED, Ejaz; BHATIA, Shishir; NADARAJAN, Anttha; RAVINDRAN, Balaraman; TICKLE, Alan B.; VIJAYASARATHY, R. **Detection and Mitigation of High-Rate Flooding Attacks.** In: RAGHAVAN, S. V.; DAWSON, Ed (Eds.). *An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks: Critical Information Infrastructure Protection*. New Delhi: Springer India, 2011. p. 131-178. DOI: https://doi.org/10.1007/978-81-322-0277-6_5.

MOULIKA, G.; PALANISAMY, P. Simulation and modeling of a robust cybersecurity system for next-generation manufacturing execution. Engineering ResearchExpress, v. 6, n. 4, p. 045425, 2024. DOI: https://doi.org/10.1088/2631-8695/ad8b09.