

Analysis of Resource Exhaustion Attacks on IoT and Edge Computing Networks in Modern Infrastructures

Constantin-Alin COPACI, Dorina-Luminița COPACI

Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest,
Romania

constantin.copaci@stud.etti.upb.ro, dorina.copaci@upb.ro

Abstract

The rapid proliferation of Internet of Things (IoT) devices and the edge computing paradigm has led to the emergence of new classes of cyberattacks that no longer primarily target cryptographic mechanisms or communication interception, but rather exploit the resource constraints of distributed nodes. This paper analyzes Resource Exhaustion attacks on IoT and edge networks, highlighting how compromised nodes can cause severe functional degradation using only legitimate traffic and commands. A conceptual and mathematical model of the attack is proposed, followed by a discussion on its security impact and modern mitigation mechanisms.

Index terms: IoT, Edge Computing, Resource Exhaustion, Firmware Malware, Network Security, Modern Attacks

References

- [1]. A.A. Laghari, H. Li, A.A. Khan et al., Internet of Things (IoT) applications security trends and challenges, *Discover Internet of Things*, vol. 4, art. 36, 2024.
- [2]. T. Rajmohan, P.H. Nguyen, and N. Ferry, "A decade of research on patterns and architectures for IoT security", *Cybersecurity*, vol. 5, art. 2, 2022.
- [3]. P.P. Jayaraman, et al., "Edge Computing for IoT: A Secure and Scalable Framework," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4450-4465, May 2020.
- [4]. L. Zhang, M. Kumar, and R. Patel, „Edge Computing and IoT Security Simulation in MATLAB/Simulink”, *IEEE Internet of Things Journal*, vol. 12, nr. 4, pp. 3012-3025, April 2025.
- [5]. E. Rescorla, I. Polakis, „TLS 1.3 Adoption, Implementation Challenges, and Security Analysis”, *ACM Computing Surveys*, vol. 57, no. 3, 2025.
- [6]. S.R. Thomas, „Next-Generation Wireless Security: WPA3 and Beyond”, *Computer Networks*, vol. 240, 2024.

- [7]. A. Sullivan, J. Smith, „Mitigating Side-Channel Attacks in WPA3-Personal and Enterprise Networks”, *IEEE Access*, vol. 12, pp. 45012-45024, 2024.
- [8]. A.K. Sood, R. J. Enbody, "Targeted Attacks on IoT Devices: Resource Exhaustion and Botnet Threats," *Journal of Information Security and Applications*, vol. 54, 2020.
- [9]. S. Kumar, et al., "Resource Exhaustion Attacks in IoT Networks: Detection and Mitigation Techniques," *IEEE Access*, vol. 8, pp. 210532-210546, 2020.
- [10]. MATLAB and Statistics Toolbox Release 2021b, The MathWorks, Inc., Natick, Massachusetts, United States.
- [11]. The MathWorks, Inc., „MATLAB Documentation”, 2021. <https://www.mathworks.com/help/matlab/>.
- [12]. D. Concejal Muñoz, A. del-Corte Valiente, *A novel botnet attack detection for IoT networks based on communication graphs*, *Cybersecurity*, vol. 6, art. 33, 2023.
- [13]. N. Canavese, L. Mannella, L. Regano, C. Basile, “Security at the Edge for Resource-Limited IoT Devices,” *Sensors*, vol. 24, no. 2, art. 590, 2024.
- [14]. L. Yin, W. Chen, X. Luo, H. Yang, Efficient Large-Scale IoT Botnet Detection through GraphSAINT-Based Subgraph Sampling and Graph Isomorphism Network, *Mathematics*, vol. 12, nr. 9, art. 1315, 2024.