Journal of Science Engineering Technology and Management Science
Volume 02, Issue 07, July 2025 *ISSN: 3049-0952*
www.jsetms.com *DOI:10.63590/jsetms.2025.v02.i07.142-145*

A REVIEW OF VARIOUS EFFICIENT TECHNIQUES FOR SECURING COAP-ENABLED IOT NETWORKS

Dr. AVLN Sujith Kumar 1 , Devender Avula 2
1 Research Supervisor, Professor of Information Technology, MallaReddy University. Hyderabad, Telangana , India
2 Research Scholar, Bharatiya Engineering, Science & Technology Innovation University, Anantapur, AP, India

To Cite this Article
Dr. AVLN Sujith Kumar, Devender Avula, "A Review Of Various Efficient Techniques For Securing Coap-Enabled Iot Networks", Journal of Science Engineering Technology and Management Science, Vol. 02, Issue 07, July 2025,pp:142-145, DOI: http://doi.org/10.63590/jsetms.2025.v02.i07.pp142-145
Submitted: 05-05-2025 *Accepted: 12-06-2025* *Published: 21-06-2025*

Abstract

This review explores the evolution of IoT Intrusion Detection Systems (IDS), transitioning from traditional anomaly-based models to advanced, intelligent detection frameworks. It synthesizes findings from fifteen peer-reviewed studies focusing on graph-based neural networks, distributed learning architectures, and resource-efficient optimization techniques. The review highlights innovations like analogical training, generative model creation, ensemble-distillation methods, and protocol-specific detection strategies. It evaluates datasets including CoAP-DoS and other benchmarks to assess detection accuracy. The study concludes that modern IDS technologies are becoming protocol-adaptable and more intellectually robust, aiming to balance computational performance, detection precision, and effective protection across diverse and resource-constrained IoT network environments.

I. INTRODUCTION

The rapid growth of IoT technologies has transformed information and communication systems, driving adoption in smart homes, transportation, grids, and healthcare. Advancements in sensors, cost control, and process optimization have expanded IoT use. However, resource-constrained devices face computing, communication, and congestion challenges. These issues lead to higher latency, energy use, and reduced performance. As a result, interest in efficient, low-resource communication methods is rising. Specialized protocols aim to enhance energy savings, resource management, and security. While TCP and UDP are standard transport protocols, they often fall short for IoT needs, prompting a shift toward lightweight, application-layer M2M communication protocols.

CoAP is a leading lightweight application-layer protocol tailored for resource-constrained IoT devices on low-energy networks. As a simplified version of HTTP, it maintains core structure while reducing bandwidth and energy use. Despite its efficiency, CoAP faces limitations in congestion control and security, making it vulnerable in high-traffic or large-scale deployments. With IoT adoption increasing, vast sensor networks generate continuous data flows, raising monitoring demands. Since similar traffic patterns can indicate normal or malicious behavior, advanced analytical techniques are essential. These methods help detect threats in ambiguous IoT traffic, ensuring more reliable and secure communication within constrained network environments.

Security in IoT environments demands Intrusion Detection Systems (IDSs), primarily signature-based and anomaly-based. Signature-based IDSs rely on known attack patterns, while anomaly-based systems detect deviations in network behavior, identifying new threats. Machine learning (ML) enhances anomaly-based IDSs by learning network patterns and identifying breaches. Detection performance varies with ML techniques: supervised, unsupervised, semi-supervised, reinforcement, or active learning. However, supervised ML IDSs face challenges due to the lack of accurately labeled IoT traffic datasets, especially for CoAP protocol operations. Real-world IDS evaluation requires datasets tailored to the constraints of wireless sensor networks and IoT-specific protocols for realistic and effective testing.

Preliminaries

This section outlines the Constrained Application Protocol (CoAP) and its role in IoT security via Intrusion Detection Systems (IDS). CoAP is a lightweight, UDP-based protocol enabling RESTful communication for constrained IoT devices, using HTTP-like methods and binary compression for efficiency. However, its minimal design creates vulnerabilities to spoofing, flooding, and replay attacks. IDSs monitor CoAP traffic to detect anomalies and intrusions using heuristic and machine learning techniques. These systems must operate with low resource consumption while maintaining high accuracy, as CoAP devices run under strict traffic and power constraints, requiring efficient and responsive IDS implementations for effective threat detection.

CoAP in IoT

CoAP is a lightweight, application-layer protocol designed by the IETF CoRE group for resource-constrained IoT devices. It enables RESTful communication using HTTP-like methods (GET, POST, PUT, DELETE) over UDP, offering low-bandwidth, energy-efficient communication ideal for lossy networks. CoAP uses binary encoding for reduced message size and supports asynchronous messaging via confirmable and non-confirmable types. Features like /.well-known/core aid resource discovery, while the Observe option enables real-time updates without constant polling. CoAP secures data with DTLS, though session management is challenging for low-resource devices. Its efficient design makes CoAP well-suited for flexible, secure IoT deployments in constrained environments.

CoAP supports multicast, enabling efficient message delivery to multiple devices—useful for synchronized sensors and software updates—unlike MQTT, which lacks native multicast. CoAP also uses proxies and caching to reduce device load and traffic. Compared to HTTP and MQTT, CoAP offers RESTful interaction, low overhead via UDP, and better suitability for constrained environments. However, it lacks built-in session management, has fewer development tools, and faces challenges with DTLS on low-power devices. Despite limitations, CoAP’s application-layer design aids anomaly detection in IDSs. Ongoing research focuses on improving CoAP's reliability, security, and scalability for smart cities, healthcare, and industrial IoT systems.

IDS for CoAP-IOT

The proposed IDS architecture is designed for CoAP-based IoT networks, functioning efficiently on constrained, low-power nodes. It features layered components: data acquisition gathers CoAP message types (CON, NON, ACK, RST), while preprocessing analyzes message frequency, payload size, address data, response time, and retransmissions. The detection engine uses signature, anomaly, and hybrid detection methods—enhanced by machine and deep learning—to identify threats like DoS, spoofing, and malformed requests. A decision-making module triggers countermeasures and alerts. Logging and updates ensure threat signature maintenance. The system's modular, lightweight, and scalable design supports adaptability across diverse CoAP-driven IoT environments.

In a CoAP-based IoT system, data is transmitted, monitored, and analyzed to detect suspicious activities efficiently. IoT devices initiate this process using CoAP via smart sensors and actuators. CoAP's lightweight framework enables real-time monitoring through GET/POST requests and message encoding. Messages are structured within the CoAP stack and transmitted via UDP. A Packet Capture Module monitors or intercepts traffic to detect anomalies during system exchanges. This module captures all CoAP messages, aiding in intrusion detection. The Feature Extraction Engine then processes these raw packets, extracting key attributes necessary for analyzing network behavior and identifying potential threats.

Recent Studies on IDS for CoAP-IoT

Intrusion detection in IoT evolves from classic anomaly detection to advanced machine learning and federated learning. A review of 15 key papers, despite limited access, reveals notable approaches. Granjal et al. (2018) use lightweight statistical models for CoAP-based WSNs. Mathews et al. (2022) introduce CoAP-DoS for IDS training. Lo et al. (2022) propose E-GraphSAGE using Graph Neural Networks. Sáez-de-Cámara and Shen (2023–2024) support federated learning for privacy-preserving IDS. Belarbi (2023) confirms its success in distributed networks. GANs (Ferdowsi & Saad, 2019), optimization (Sharma, 2024), reinforcement learning (Gueriani, 2023), and neural-growth methods (Fatani, 2023) all enhance IDS adaptability and performance.

Recent research highlights advanced IDS strategies for CoAP-based IoT systems. Almeghlef et al. (2023) focus on CoAP-layer DoS attacks, while Alsulami et al. (2023) develop IDS tailored for CoAP. Kipongo et al. (2023) compare RPL and AODV protocols for WSN IDS design. Yadav et al. (2022) integrate deep learning with 5G IoT, and Awajan (2023) builds deep learning-based IDS adapted to IoT. Granjal et al. (2018) introduced lightweight, context-aware anomaly detection. Mathews et al. (2022) created the CoAP-DoS dataset for benchmarking. Lo et al. (2022) present E-GraphSAGE, a GNN framework that leverages IoT's relational structure for accurate intrusion detection.

II. RESEARCH GAPS

A key research gap in IoT intrusion detection is the lack of diverse, standardized datasets tailored to specific protocols. While Mathews et al. (2022) introduced the CoAP-DoS dataset, most studies rely on limited or unrealistic data, hindering reproducibility and model comparison. There's a pressing need for multi-layer datasets (e.g., CoAP, MQTT, RPL) that reflect real-world traffic and attack scenarios. IDS development also struggles with non-IID data and device diversity, as noted by Sáez-de-Cámara (2023) and Shen (2024). Although some federated models perform well in simulations, they often fail in real environments, highlighting the need for adaptable, resource-efficient IDS frameworks.

Designing IoT security solutions requires balancing strong performance with the limited capabilities of embedded devices. Deep learning models by Lo and Awajan (2022–2023) show high accuracy but demand excessive resources, limiting deployment on constrained hardware. Current IDS solutions lack the low-power, real-time response needed for edge devices. Optimization techniques like model pruning, quantization, and real-time feature selection are essential for efficient on-device inference. While GANs and deep reinforcement learning have been explored (Gueriani, 2023; Ferdowsi & Saad, 2019), real-time adaptation remains limited. Continuous learning IDS frameworks are urgently needed to autonomously adapt to evolving threats using live traffic data.

III. CONCLUSION

The current landscape of IDS research in IoT demonstrates a strategic shift toward decentralized, learning-driven, and protocol-sensitive detection mechanisms that reflect the complexities of modern network environments. Despite notable progress in areas such as federated learning, deep reinforcement learning, and graph-based modeling, several critical gaps persist—including limited availability of comprehensive datasets, generalizability across heterogeneous devices, and the lack of lightweight models suited for real-time inference. Furthermore, adaptive mechanisms capable of handling evolving threats with minimal manual intervention remain underdeveloped. Future research must prioritize the development of scalable, efficient, and context-aware IDS frameworks, supported by standardized evaluation protocols and realistic testbeds, to ensure robust security in the ever-expanding IoT ecosystem.

REFERENCES

[1] Donta, P.K.; Srirama, S.N.; Amgoth, T.; Annavarapu, C.S.R. Survey on recent advances in IoT application layer protocols and machine learning scope for research directions. Digit. Commun. Netw. 2021, 8, 727–744. [CrossRef]

[2] RFC 7252 Constrained Application Protocol. Available online: https://coap.technology/ (accessed on 17 October 2022).

[3] Rahman, R.A.; Shah, B. Security analysis of IoT protocols: A focus in CoAP. In Proceedings of the 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, 15–16 March 2016; pp. 1–7. [CrossRef]

[4] Fahim, M.; Sillitti, A. Anomaly Detection, Analysis and Prediction Techniques in IoT Environment: A Systematic Literature Review. IEEE Access 2019, 7, 81664–81681. [CrossRef]

[5] Shafiq, M.; Thakre, K.; Krishna, K.R.; Robert, N.J.; Kuruppath, A.; Kumar, D. Continuous quality control evaluation during manufacturing using supervised learning algorithm for Industry 4.0. Int. J. Adv. Manuf. Technol. 2023, 1–10. [CrossRef]

[6] Bhuyan, M.H.; Bhattacharyya, D.K.; Kalita, J.K. Towards Generating Real-life Datasets for Network Intrusion Detection. Int. J. Netw. Secur. 2015, 17, 683–701.

[7] Chen, H.; Xiong, Y.; Li, S.; Song, Z.; Hu, Z.; Liu, F. Multi-Sensor Data Driven with PARAFAC-IPSO-PNN for Identification of Mechanical Nonstationary Multi-Fault Mode. Machines 2022, 10, 155. [CrossRef]

[8] Centro de InvestigaciónenTecnoloxías da Información e as Comunicacións de Galicia. Available online: https://www.citicresearch.org/ (accessed on 30 October 2022).

[9] Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D.; Elovici, Y. N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. IEEE Pervasive Comput. 2018, 17, 12–22. [CrossRef]

[10] Mirsky, Y.; Doitshman, T.; Elovici, Y.; Shabtai, A. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. arXiv 2018, arXiv:1802.09089.