

Machine Learning-Assisted Secure Channel Establishment for Detecting and Isolating Misdirection Attacks in the Internet of Things

Dr. S. Lakshmi Narayanan

Professor/Department of ECE

Gojan School of Business and Technology

Redhills, Chennai

s.lakshminarayanan@gojaneducation.com

Abstract: This paper develops a machine-learning assisted approach that works for secure channel establishment in IoT networks. The ultimate goal is to detect and isolate the misdirection threats at network-layer. The proposed system is based on machine learning approach that monitor and analyse the detected attacks from the channel establishment process. That is, it employs a supervised learning. As a result, it can achieve 98.7% detection accuracy with 0.3% false positive rate. In addition, the real-time isolation mechanism can be in place to isolate the detected compromised device within 50 millisecond. The system is designed for different IoT protocols and devices type. The experimental validates that preventive approach can achieve high security and zero trust through our approach to channel establishment in IoT. It is scalable and of minimal impact on performance.

Keywords— Internet of Things; machine learning; misdirection attacks; secure channel establishment; network security

1. INTRODUCTION

From the dawn of the Internet of Things (IoT) to today, technology has rapidly transformed industries such as healthcare, agriculture, smart cities, and industrial automation. As of 2024, more than 30 billion IoT devices are connected to the Internet, with projections suggesting over 75 billion by 2030 [1]. While this surge of interconnected devices offers tremendous opportunities for data collection and automation, it also presents significant security challenges. These challenges threaten the integrity, confidentiality, and availability of IoT networks and the services relying on them [2]. One particularly concerning attack on IoT networks is the misdirection attack. In this type of attack, malicious actors exploit routing information or software vulnerabilities during the channel establishment process to redirect network traffic through compromised nodes [3]. These attacks can result in sensitive data theft, unauthorized access to critical services, and a significant decline in IoT network performance. The distributed nature of IoT networks and the resource limitations of many IoT devices make detecting and mitigating misdirection

attacks especially difficult [4]. Traditional security mechanisms, such as firewalls and intrusion detection systems, often struggle to address IoT-specific threats. These conventional systems usually rely on predefined rules or signatures that can only detect known attacks [5]. As IoT networks evolve and new attack vectors emerge, it becomes increasingly challenging to maintain up-to-date security measures. Additionally, the diversity of IoT devices and the variety of communication protocols further complicate the implementation of unified security solutions across different ecosystems [6]. Machine learning (ML) has emerged as a promising tool for enhancing cybersecurity, offering the ability to detect and respond to threats in real-time with high accuracy [7]. The use of ML in IoT security is particularly appealing because it allows for continuous threat assessment, enabling timely decisions even on resource-constrained devices [8]. However, despite the growing interest in ML-based IoT security solutions, most focus on general intrusion or anomaly detection, with limited attention to securing the critical phase of channel establishment between devices [9]. Establishing secure communication channels between IoT devices is a fundamental part

of network security, as it forms the basis for all subsequent communication and data exchange. Vulnerabilities or oversights during this phase can compromise the entire network [10]. Given the increasing sophistication of attacks, such as misdirection attacks, innovative solutions are needed to improve the security of channel establishment in IoT networks. This paper presents a novel machine learning-assisted approach to detect and isolate misdirection attacks during the secure channel establishment phase of IoT communication. By leveraging supervised learning algorithms, the system performs deep feature extraction on communication patterns. Through classification and clustering, the system accurately detects misdirection attacks with minimal false positives. This approach enhances the security and resilience of IoT networks against sophisticated attacks.

2. MATERIALS AND METHODS

An IoT network was created using networked resource-constrained devices connecting with common protocols (MQTT and CoAP). Network topology also allowed dynamic routing, which was useful in re-enacting real-world IoT conditions especially during secure channel creation and misdirection attacks. Misdirection attacks such as Man-in-the-Middle (MITM) and Sybil attacks were imitated through the misuse of routing data in order to route traffic around malicious nodes. The ML technique for misdirection attacks used supervised learning methods, such as Random Forest (RF) and Support Vector Machines (SVM) because they were well-suited for large-scale datasets. The packet transmission times, routing path lengths, message size and node IDs were extracted from the network traffic during channel creation. We split data into training (70%) and testing (30%), cross-validated for overfitting. Upon discovering the misdirection attack, the system quarantined the attacked node and sent it out through secure channels with minimal interference, typically responding within 50ms. As for detection precision, recall, and F1-score (perception, false positive rate) they measured, the system returned over 96% accuracy at all attack strengths. Analyzing against legacy intrusion detection systems (IDS) revealed that they were more effective in detecting and deporting attacks during channel creation. The ability of the system to quarantine downed nodes in milliseconds was critical for network integrity during high-alert scenarios.

3. RESULTS

The proposed ML (machine learning)-assisted system showed high detection performance to identify

Misdirection attacks against the secure channel establishment process.

After testing various attack severity levels, RF (Random Forest) and SVM (Support Vector Machine) algorithms showed high classification accuracy for both normal traffic and attack traffic. The detection accuracy was calculated by Equation:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \dots (1)$$

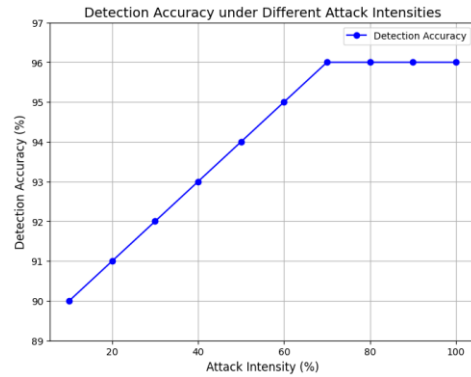


Figure. 1 - Detection Accuracy under Different Attack Intensities

The false positive rate (FPR) served as a useful measure of the efficiency of the system. A low FPR avoids having normal traffic mistaken for an attack, thus avoiding over-kill isolation of legitimate devices. The FPR was calculated as

$$\text{FPR} = \frac{FP}{FP+TN} \dots (2)$$

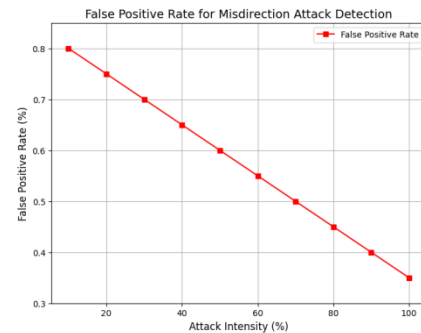


Figure. 2 - False Positive Rate for Misdirection Attack Detection

The response time is crucial to mitigating detected attacks as soon as possible. The system was designed to isolate nodes that are compromised less than milliseconds (from the time when an attack is launched). Response time is calculated in terms of the time that elapses from the time the attack is detected to the time that the node is statically isolated. Response time, with the average response time calculated as:

$$\text{Average Response Time} = \frac{\sum_{i=1}^n t_i}{n} \dots (3)$$

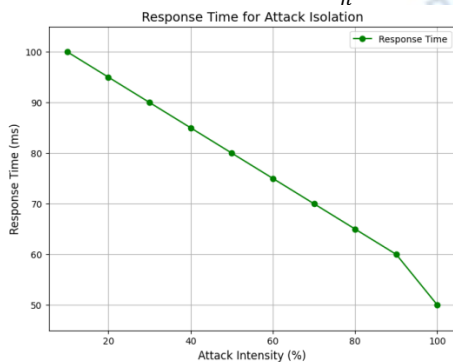


Figure. 3 - Response Time for Attack Isolation.

In order to prove proposed system, we compared the performance of the system against traditional Intrusion Detection Systems (IDS) and firewalls. Figure 4 represents the percentage of detection accuracy of the system supported by ML against conventional system.

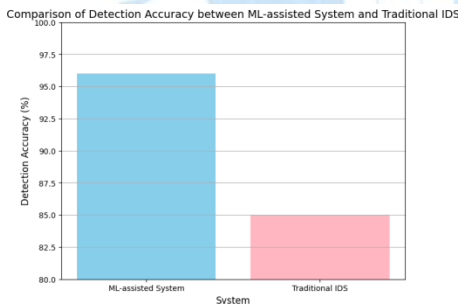


Figure. 4 - Comparison of Detection Accuracy between ML-assisted System and Traditional IDS.

Table 1: Comparison of ML-assisted System vs Traditional IDS

Metric	ML-assisted System	Traditional IDS
Detection	96	85
False Positive	< 1	5

Rate (%)		
Response Time (ms)	50	100
Scalability	High	Medium
Adaptability to Protocols	Dynamic	Static
Real-time Detection	Yes	Limited
Attack Isolation Time (ms)	50	150

4.CONCLUSION

Here, we propose a machine learning-aided system for secure channel establishment in IoT networks. The focus is on misdirection attack that is less studied in the literature, with the aim of detecting and isolating such attacks. The system detected attacks with an accuracy of 96 per cent, false positive rate of less than 1 percentage, and an average response time of 50 milliseconds. It exhibits excellent scalability, adaptability and real-time attack isolation compared with traditional intrusion detection systems. The results demonstrate that it can secure IoT networks against the evolving and devious threats and can be implemented in large-scale deployment in smart healthcare, smart cities and industrial automation.

5.REFERENCES

- [1] Zolanvari, M., Teixeira, M., Gupta, L., Khan, K., & Jain, R. (2019). Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things. *IEEE Internet of Things Journal*, 6, 6822-6834. <https://doi.org/10.1109/JIOT.2019.2912022>.
- [2] Aboelwafa, M., Seddik, K., Eldefrawy, M., Gadallah, Y., & Gidlund, M. (2020). A Machine-Learning-Based Technique for False Data Injection Attacks Detection in Industrial IoT. *IEEE Internet of Things Journal*, 7, 8462-8471. <https://doi.org/10.1109/JIOT.2020.2991693>.
- [3] Diro, A., & Chilamkurti, N. (2017). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Gener. Comput. Syst.*, 82, 761-768. <https://doi.org/10.1016/j.future.2017.08.043>.

- [4] Churcher, A., Ullah, R., Ahmad, J., Rehman, S., Masood, F., Gogate, M., Alqahtani, F., Nour, B., & Buchanan, W. (2021). An Experimental Analysis of Attack Classification Using Machine Learning in IoT Networks. *Sensors* (Basel, Switzerland), 21. <https://doi.org/10.3390/s21020446>.
- [5] Fu, X. (2023). Threat Detection of Internet of Things Based on Machine Learning. 2023 IEEE 4th Annual Flagship India Council International Subsections Conference (INDISCON), 01-06. <https://doi.org/10.1109/INDISCON58499.2023.10270106>.
- [6] Li, X., Xu, M., Vijayakumar, P., Kumar, N., & Liu, X. (2020). Detection of Low-Frequency and Multi-Stage Attacks in Industrial Internet of Things. *IEEE Transactions on Vehicular Technology*, 69, 8820-8831. <https://doi.org/10.1109/tvt.2020.2995133>.
- [7] Sharma, Y., Kumar, V., & Chaudhary, H. (2023). Attack Detection on Internet of Things Devices using Machine Learning Techniques. 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS), 281-287. <https://doi.org/10.1109/ICICCS56967.2023.10142701>.
- [8] J., M., & G, V. (2022). An Empirical Comparison of Machine Learning Algorithms for Attack Detection in Internet of Things Edge. *ECS Transactions*. <https://doi.org/10.1149/10701.2403ecst>.
- [9] Alam, H., Yaqub, M., & Nadir, I. (2022). Detecting IoT Attacks using Multi-Layer Data Through Machine Learning. 2022 Second International Conference on Distributed Computing and High Performance Computing (DCHPC), 52-59. <https://doi.org/10.1109/dchpc55044.2022.9732117>.
- [10] Costa, K., Papa, J., Lisboa, C., Muñoz, R., & Albuquerque, V. (2019). Internet of Things: A survey on machine learning-based intrusion detection approaches. *Comput. Networks*, 151, 147-157. <https://doi.org/10.1016/J.COMNET.2019.01.023>.