RESEARCH ARTICLE OPEN ACCESS

Network Layer Threats in IoT Security: Challenges and Countermeasures

Abdullah M. A. Alzafiri*
**(Industrial Institute -Shuwaikh, Public Authority of Applied Education and Training, Kuwait)*

ABSTRACT
Internet of Things (IoT) is developing billions of physical devices into the digital space and allows for automated real-time data sharing across multiple industries, bringing unprecedented convenience and efficiency along with undoubtedly and arguably complex security risks, particularly at the network layer of the IoT architecture, the layer that handles the routing, forwarding, and exchanging of information. This paper analyzes the most common threats aimed at the network layer of IoT domains such as sinkhole, Sybil, wormhole, selective forwarding, and denial of service (DoS) attacks. Furthermore, it examines the inherent vulnerabilities found in various IoT realms, proposing security protocols and counter-measures that have been adopted in the IoT space and finally looks at research paradigms, trends, and future directions. This paper will add to the understanding of security methods for the network layer of IoT as the IoT becomes more intertwined [1][2].

Keywords *- IoT, Network layer, Routing Attacks, IoT security, Intrusion Detection, Secure Routing, Trust Management*

Date of Submission: 10-04-2025 Date of acceptance: 23-04-2025

I. INTRODUCTION

The rapid adoption of Internet of Things (IoT) devices are changing the modern digital ecosystem by enabling smarter environments through data collection and real-time digitalization. IoT applications in health care, transportation, smart cities, and agriculture are enabled through conversation across devices orchestrated by the network layer of the IoT framework. The network layer as defined in the IoT architecture is responsible for establishing appropriate routing addressing tasks and communication of packets inside a resource constrained and often ad hoc based network environments. Despite its important role in IoT, the network layer are the most vulnerable of the IoT layers, due to lightweight protocols and resource constrained devices [1][2]. These threats not only affect individual devices, but entire groups of devices and networks, and it is important to understand the types of attacks possible and to what level can they compromise our networks, if the IoT DevOps world continues to grow. This study explores comprehensively the nature of these threats with their implications, and mitigations that can be taken.

II. THE NETWORK LAYER IN IOT ARCHITECTURE

The Network Layer is responsible for end-to-end data delivery, forwarding packets, and managing routes. 6LoWPAN, RPL, Zigbee, and Thread protocols are common approaches that IoT workers employ to enable communication between heterogeneous devices. These protocols were developed intentionally for low-power, lossy networks and mostly have no or limited built-in security properties [1]. For example, RPL uses rank-based routing that attackers can exploit to compromise the topology when an adversary can change their rank value of their node for routing purposes. Additionally, low power-considerations also result in very weak and/or very limited encryption and identity validation mechanisms [2].

For many IoT devices, communication is completed via mesh networking in which data packets are relayed through intermediary nodes before reaching the final, intended destination. The lack of strong cryptographic protections and also dynamic topology make it equally easy, for an attacker to extract benign routing information or device information (e.g. impersonate a legitimate device) [7]. Further making any intrusion detection or incident response, more complex is that these networks often operate unattended [5].

III. MAJOR NETWORK LAYER THREATS.

Sinkhole Attacks: Sinkhole attacks leverage the routing protocols in an IoT network to converge all your node's traffic to a malicious or adversarial node by offering a false representation of being the shortest or most reliable path, then the attacker intercepts that data, they can and may either drop, manipulate, or analyze it. In RPL based IoT networks, attackers use the same paradigm of exploiting rank based routing with malicious nodes altering their rank value to claim to be closer to the root node and steal the routing paths from the benign nodes within that network [2].

Sybil Attacks: A Sybil attack occurs when one node injects multiple fake identities into the network. This is detrimental to trust-based routing, any voting system flexibility, or redundancy. In scenarios like smart grids or healthcare IoT systems, these attacks can determine decision-making conduct, whether that be rerouting traffic or cascading denial of service attacks [3].

Wormhole attacks: Wormhole attacks happen when two colluding nodes establish a private link or "'tunnel'" between two nodes in a network. When packets are captured at one end of the tunnel, the colluding nodes can replay the packets on the other end, forming a shortcut. The routing protocols can become misled and forward packets through the tunnel, circumventing legitimate routing and breaching the integrity of the network [4].

Selective forwarding: Selective forwarding attacks are a more subtle denial of service attack where the malicious node forwards some data packets while dropping others while falsely representing that it detected the packets. These class of denial of service attacks are also difficult to detect particularly on lossy networks that can encounter natural packet drops [5].

Denial of Service (DoS): DoS attacks at the network layer are particularly effective in the IoT network especially where there is limited bandwidth and scarce device resources. Attackers can overload routing messages or repeatedly trigger DODAG Information Object (DIO) broadcasts in the RuP that exploit vulnerabilities of MAC-layer [6].

IV. CHALLENGES IN SECURING THE IOT NETWORK LAYER

IoT network has security challenges base on a few core defining characteristics:

Resource constraints: IoT devices generally have very limited memory, battery life and processing power. Many device can practically not operate cryptographic protocols, like TLS or IPsec [1].

Heterogenous and interoperability: all devices must be interoperable easily with respect to other manufacturer devices that may support different communication standard. This inconsistency limits the implementation of shared security frameworks [7].

Dynamic Topologies: Devices within the IoT typically are dynamic with devices regularly joining or leaving the network creating a need for ongoing adjustments in routing and trust relationships [2].

Physical Exposure: Many IoT nodes are installed in public or remote areas and thus are exposed to physical attacks [5].

Lack of standardization: Security frameworks and architecture for IoT/deployment are being developed. Differences in vendor implementation abilities add complexity to the process of deployment and compliance and also have the potential for complications during deployment [6].

V. EXISTING RESPONSES

Researchers and practitioners have developed a number of methods to protect the IoT network layer against known exploits. These methods include:

Lightweight Cryptography: (ECC, PRESENT, and SPECK): algorithms intended for low resource environments [6];

Security-Routing Protocols: (i. e. , enhanced RPL, Trust-RPL, or Secure-RPL (SRPL)): which provide monitoring of node behavior, validating routing metrics, and trust [2]; Trust based systems which can integrate metrics from node behavior (i. e. , packet forwarding, and engagement in control messages [7].

Intrusion Detection Systems (IDS): which can run on edge or centralized nodes and employ detection anomalies based upon statistical, or machine learning detection of abnormal routing patterns or packet drops due to attacks [8].

Blockchain Technology: which provides immutable log data or decentralized trust, with lightweight blockchains like IOTA and Nano providing secure identify and access without centralized servers [9].

Reputation Systems: which can run alongside trust models. They enable nodes to assess peers on the basis of their past experiences. [3]

VI. CASE STUDIES AND REAL-WORLD INCIDENTS

Mirai Botnet: The Mirai malware turned thousands of insecure IoT devices into a full-fledged botnet to launch DDoS attacks against DNS providers and websites. Although Mirai primarily exploited weaknesses at the application layer, Mirai also demonstrated how a poorly authenticated identity for devices and no authentication for routing devices led to quickly replicating the botnet. [8]

Smart Grid Routing Attack: Simulations conducted as research have indicated that routing attacks, especially on RPL, could cause lost data or depletion of energy in smart grid networks. [2]

Medical IoT Networks: It is always critical for healthcare to receive sensor data in a timely manner. A case study published in 2020 demonstrated that attacks in wearable networks using selective forwarding led to improperly monitored patients, which could result in undelayed medical responses. [5]

VII. FUTURE DIRECTIONS

Securing the IoT at the network layer will remain an open research challenge. Future-oriented approaches worth pursuing include:

Deploying Artificial Intelligence at the Edge: lightweight AI models are now available, enabling IoT nodes to detect anomaly in real time without latency. Federated learning enables training collaboratively without having to centralize data. [10]

Quantum Resistant Algorithms: Post-quantum cryptography (PQC) is being developed to replace cryptography methods that quantum computers could break. [10]

Context-Aware Security Policies: Updating adaptive, contextually relevant policies by monitoring node activity, networks or environment can augment learning trust and disrupt performance fraud. [7]

Hybrid Security Frameworks: using two or more methods and including the schemes of cryptography, trust and usage of blockchain could yield sound protection. [9]

Cross-layer defense integration: designing security measures should not be limited to one layer (physical, MAC, network, application), but incorporate an integrated approach to security measures [6].

VIII. CONCLUSION

At the network layer, threats to IoT environments are among the most harmful because of their ability to manipulate routing, degrade communication, and enable further attacks. These types of attacks impact performance as well as trust in the system. The reality of IoT's unique limitations- constrained resources, experimental protocols or mix of protocols, and decentralized topology- means the security measures put in place must be adaptive or not easily adaptable. A hybrid model of lightweight cryptography, trust management, secure routing, along with decentralized trust frameworks, could also provide least resistance to compromise through layers of security. Future research should focus on new lines of defense with AI, standardization, and quantumsafe protocols, even as IoT continues to be more pervasive and complex.

REFERENCES

[1]. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164.

[2]. Zhou, W., Zhang, Y., Liu, P., & Ning, J. (2018). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. IEEE Internet of Things Journal, 6(2), 1606–1616.

[3]. Le, A., Loo, J., Lasebae, A., Aiash, M., & Luo, Y. (2016). The impact of rank attack on network topology of routing protocol for low-power and lossy networks. IEEE Sensors Journal, 16(12), 4725–4736.

[4]. Douceur, J. R. (2002). The Sybil attack. In International Workshop on Peer-to-Peer Systems (pp. 251–260).

[5]. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279.

[6]. Liu, B., Xu, L., Xu, Y., & Zhang, Y. (2021). A lightweight ECC-based authentication protocol for IoT devices. IEEE Internet of Things Journal, 8(3), 1510–1518.

[7]. HaddadPajouh, H., Dehghantanha, A., Khayami, R., & Choo, K. K. R. (2018). A survey on Internet of Things security: Requirements, challenges, and solutions. Computers & Security, 89, 123–147.

[8]. Kolias, A., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80–84.

[9]. Novo, O. (2018). Blockchain meets IoT: Architecture for scalable access management. IEEE Internet of Things Journal, 5(2), 1184–1195.

[10]. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concepts and applications. ACM TIST, 10(2), 1–19.