ISSN 2349-0292
Impact Factor 3.802
GLOBAL JOURNAL OF ADVANCED ENGINEERING TECHNOLOGIES AND SCIENCES

SECURE ROUTING PROTOCOLS FOR INTERNET OF THINGS (IOT) NETWORKS

Jyoti Tiwari, Abhishek Barche
Assistant Professor, Institute of Computer Application, Sage university indore
Email: jyotitiwari.992@gmail.com
Assistant Professor, Institute of Computer Application, Sage university indore
Email: barches3410@gmail.com

ABSTRACT

The exponential growth of the Internet of Things (IoT) has revolutionized communication networks, enabling intelligent applications across various domains. However, the decentralized and resource-constrained nature of IoT networks introduces significant security and privacy concerns, especially in routing mechanisms. This paper provides a comprehensive analysis of secure routing protocols designed for IoT networks. It explores the threats and challenges unique to IoT routing, evaluates existing secure routing protocols, and discusses emerging trends and future directions for achieving robust and scalable security in IoT communication systems.).

KEYWORDS: IoT, secure routing, trust-based protocols, cryptographic protocols, RPL, cyber-attacks, resource constraints, blockchain, energy-efficient security, lightweight encryption.

INTRODUCTION

The Internet of Things (IoT) is redefining the digital landscape by enabling the integration of everyday objects into interconnected, intelligent environments. From smart cities and connected vehicles to industrial automation and precision agriculture, IoT is facilitating seamless data exchange and real-time decision-making at an unprecedented scale. According to recent estimates, the number of connected IoT devices is projected to surpass 30 billion by 2030, reflecting the widespread adoption and critical role of this technology in modern society.

Despite its transformative potential, IoT also introduces substantial technical and security challenges, especially in the domain of networking and communication. Unlike traditional computing systems, IoT devices are typically resource-constrained — characterized by limited computational power, energy capacity, and memory. These constraints make it impractical to implement conventional security mechanisms directly, thereby exposing IoT networks to a wide range of vulnerabilities.

Routing, a fundamental aspect of network communication, is particularly susceptible to security threats in IoT environments. In these networks, routing protocols must efficiently discover and maintain optimal paths between devices while minimizing energy usage and coping with dynamic topologies. At the same time, they must protect against adversarial behaviors such as data interception, route manipulation, and packet dropping — all of which can severely compromise network integrity and availability.

Traditional routing protocols, designed primarily for wired or mobile ad hoc networks, fall short in meeting the stringent security and performance requirements of IoT systems. This has led to the development of specialized **secure routing protocols** that aim to balance **efficiency, resilience, and lightweight cryptographic functionality**. These protocols often incorporate trust evaluation, cryptographic techniques, blockchain mechanisms, and bio-inspired algorithms to enhance security without overwhelming device capabilities.

The objective of this paper is to provide a comprehensive overview of secure routing protocols tailored for IoT networks. We begin by identifying key security challenges inherent to IoT routing and then present a taxonomy of existing secure routing approaches, including trust-based, cryptography-based, AI-driven, and blockchain-supported protocols. Additionally, the paper evaluates performance metrics, reviews relevant case studies, and highlights emerging research directions aimed at strengthening the security posture of future IoT communication systems.

ISSN 2349-0292
Impact Factor 3.802

LITERATURE REVIEW

Numerous researchers have explored secure routing protocols tailored to the unique requirements of IoT:

- **Raza et al. (2013)** compared IPsec and link-layer security for 6LoWPAN networks, concluding that while IPsec offers strong security, its overhead is unsuitable for resource-constrained nodes.
- **Tsao et al. (2017)** provided a detailed threat analysis of RPL-based networks, identifying attack vectors such as sinkhole, wormhole, and Sybil attacks in Low-Power and Lossy Networks (LLNs).
- **Tripathi et al. (2020)** conducted a survey of secure routing approaches, highlighting trust-based and hybrid models as promising methods for attack mitigation without significant energy cost.
- **Ali et al. (2019)** proposed a secure and energy-efficient routing protocol based on node reputation and trust metrics, demonstrating resilience against selective forwarding and blackhole attacks.
- **Dorri et al. (2017)** presented a blockchain-based architecture for secure communication in IoT environments, focusing on privacy and trust management in smart homes.

These studies collectively suggest that a one-size-fits-all approach is impractical for IoT routing security. Instead, protocol designs must consider trade-offs between energy efficiency, scalability, and the ability to counteract multiple threat types.

SECURITY CHALLENGES IN IOT ROUTING

Resource Constraints

IoT devices typically have limited computational power, memory, and battery life, which complicates the implementation of conventional cryptographic techniques and routing protocols.

Network Dynamics

Frequent topology changes, node mobility, and intermittent connectivity demand adaptive routing solutions that can maintain security without introducing excessive overhead.

Threat Model

IoT networks face numerous threats, including:

- Sybil Attacks
- Wormhole Attacks
- Blackhole Attacks
- Selective Forwarding
- Sinkhole Attacks

CLASSIFICATION OF SECURE IOT ROUTING PROTOCOLS

Trust-Based Routing Protocols

- **T-RPL**: Dynamic trust evaluation integrated into RPL.
- **TRPL-S**: Combines trust scores and link reliability for route optimization.

Cryptography-Based Protocols

- **S-RPL**: Incorporates symmetric cryptography into RPL routing.
- **LEAP+**: Lightweight key management for secure data transmission.

Bio-Inspired and AI-Driven Protocols

- **AntHocNet-Secure**: Ant-colony optimization with anomaly detection.
- **RL-Secure Routing**: Adaptive learning for intelligent path selection.

Blockchain-Based Routing

- **BRPL**: Blockchain-enhanced RPL to ensure route authenticity and immutability.

EVALUATION METRICS FOR SECURE ROUTING

- Packet Delivery Ratio (PDR)
- Energy Consumption
- Latency
- Routing Overhead
- Detection Rate

CASE STUDIES

T-RPL vs S-RPL

T-RPL shows better resilience in environments susceptible to trust-based attacks, while S-RPL is more effective in safeguarding confidentiality in static topologies.

BRPL in Smart Grid Applications

While BRPL enhances transparency and auditability, latency and storage demands can increase due to blockchain overhead.

FUTURE RESEARCH DIRECTIONS

- Development of post-quantum lightweight cryptography for IoT.
- Federated learning for secure, decentralized anomaly detection.
- Cross-layer security integration for improved performance.
- Hybrid trust-cryptography-blockchain models for multi-layered security.

PROBLEM STATEMENT

The Internet of Things (IoT) is rapidly expanding, integrating billions of devices across diverse domains. However, this growth introduces critical security vulnerabilities in routing mechanisms due to the resource-constrained nature of IoT devices (limited power, memory, and computation) and the dynamic topologies of these networks. Traditional routing protocols, designed for more stable and resource-rich environments, are inadequate for ensuring secure and efficient communication in IoT systems.

IoT networks are highly susceptible to attacks such as sinkhole, Sybil, wormhole, selective forwarding, and blackhole attacks, which can compromise data integrity, confidentiality, and availability. There is a pressing need for specialized secure routing protocols that balance energy efficiency, scalability, and robust security measures tailored to the constraints of IoT.

Thus, the central problem is the design and implementation of lightweight, scalable, and attack-resilient routing protocols that can protect IoT communications against evolving threats while operating within the constraints of IoT devices.

SUMMARY

This paper acts as a survey and evaluative framework for current secure routing strategies in IoT, offering readers a structured understanding of the field, comparing the effectiveness of existing solutions, and pointing toward future research directions for more robust and adaptive IoT security systems.

CONCLUSION

Secure routing is fundamental for the reliability and success of IoT networks. Despite significant progress, trade-offs between security, performance, and energy efficiency remain unresolved. This paper highlights key secure routing protocols and their methodologies while proposing avenues for future improvements. Advancing toward scalable, lightweight, and intelligent secure routing protocols is essential to safeguard the evolving IoT ecosystem.

REFERENCES

[1] Raza, S., Seitz, L., Sitenkov, D., & Selander, G. (2013). "Security protocols for the Internet of Things." IEEE Communications Surveys & Tutorials, 15(2), 878-888.
[2] Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., & Richardson, M. (2017). "A Security Threat Analysis for RPL-based IoT Networks." RFC 7416.
[3] Tripathi, J., Bouazizi, I., & Minet, P. (2020). "A survey on secure routing in the Internet of Things: Issues and current solutions." Journal of Network and Computer Applications, 163, 102630.
[4] Ali, M. S., Dyo, V., & Harle, R. (2019). "Secure and energy-efficient data routing protocol for IoT-based wireless sensor networks." IEEE Access, 7, 26750-26761.
[5] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). "Blockchain for IoT security and privacy: The case study of a smart home." 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 618–623.
[6] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). "Internet of Things security: A survey." Journal of Network and Computer Applications, 88, 10–28.

[7] Zhang, K., Liang, X., Lu, R., & Shen, X. (2014). "Sybil attacks and their defenses in the Internet of Things." IEEE Internet of Things Journal, 1(5), 372–383.
[8] Mayzaud, A., Badel, S., Noirie, L., & Chrisment, I. (2016). "A taxonomy of attacks in RPL-based Internet of Things." International Journal of Network Security, 18(3), 459–473.
[9] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10–28. https://doi.org/10.1016/j.jnca.2017.04.002
[10] Ali, M. S., Dyo, V., & Harle, R. (2019). Secure and energy-efficient data routing protocol for IoT-based wireless sensor networks. IEEE Access, 7, 26750–26761. https://doi.org/10.1109/ACCESS.2019.2900652
[11] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 618–623). IEEE. https://doi.org/10.1109/PERCOMW.2017.7917634
[12] Mayzaud, A., Badel, S., Noirie, L., & Chrisment, I. (2016). A taxonomy of attacks in RPL-based Internet of Things. International Journal of Network Security, 18(3), 459–473.
[13] Raza, S., Seitz, L., Sitenkov, D., & Selander, G. (2013). Security protocols for the Internet of Things. IEEE Communications Surveys & Tutorials, 15(2), 878–888. https://doi.org/10.1109/SURV.2012.111412.00134
[14] Tripathi, J., Bouazizi, I., & Minet, P. (2020). A survey on secure routing in the Internet of Things: Issues and current solutions. Journal of Network and Computer Applications, 163, 102630. https://doi.org/10.1016/j.jnca.2020.102630
[15] Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., & Richardson, M. (2017). A security threat analysis for RPL-based IoT networks. RFC 7416. https://doi.org/10.17487/RFC7416
[16] Zhang, K., Liang, X., Lu, R., & Shen, X. (2014). Sybil attacks and their defenses in the Internet of Things. IEEE Internet of Things Journal, 1(5), 372–383. https://doi.org/10.1109/JIOT.2014.2344013