Volume 3, Issue 2, 2024
PP 17-20

International Journal of Futuristic Innovation in Arts, Humanities and Management (IJFIAHM)

Secure and Efficient Key Management for Dynamic Network Topologies in IoT

[1]Dr.Zubair Ahmed Khan
Assistant Professor, Department of Computer Science & Engineering, MATS School of Engineering & IT,MATS UNIVERSITY, Aarang & Raipur
zubairashrafi786@hotmail.com

2Prof (Dr.) Asha Ambhaikar
Professor, Department of Computer Science & Engineering MATS School of Engineering & IT, MATS UNIVERSITY Aarang & Raipur
drambhaikar@gmail.com

Abstract

The rapid expansion of the Internet of Things (IoT) has resulted in a significant increase in the number of interconnected devices, leading to highly dynamic and complex network topologies. This evolution introduces critical security vulnerabilities, particularly in ensuring secure communication. Effective key management is pivotal in mitigating these risks and safeguarding data integrity within such networks. This study systematically examines the challenges associated with secure and efficient key management in dynamic IoT environments. Existing methodologies are analyzed to identify their limitations, and an innovative framework is proposed to enhance security while preserving operational efficiency. The proposed framework addresses the unique requirements of IoT networks, including scalability, adaptability, and resource constraints, offering a comprehensive approach to improving key management practices.

Keywords
Internet of Things, Key Management, Secure Communication, Dynamic Network Topologies, Scalability, Resource-Constrained Systems, Data Integrity.

Introduction

The Internet of Things (IoT) comprises billions of interconnected devices, ranging from sensors to advanced smart appliances, forming an expansive and dynamic network. These networks are inherently characterized by frequent topological changes driven by device mobility, intermittent connectivity, and variable device lifecycles. In this highly dynamic context, secure key management emerges as a critical component for ensuring data integrity, confidentiality, and overall system security.

However, traditional key management schemes are often ill-suited to address the unique challenges posed by IoT environments. These challenges include the need for scalability to accommodate the continuous expansion of connected devices, flexibility to adapt to evolving network topologies, and the ability to operate within the stringent energy and resource constraints of IoT devices. Addressing these limitations requires innovative approaches that are tailored to the heterogeneous and resource-constrained nature of IoT ecosystems.

Scalability

IoT networks often involve a large number of devices. Traditional key management systems, which are designed for relatively static and smaller networks, face scalability issues when applied to IoT. Efficiently managing keys for millions of devices without compromising security is a significant challenge.

Dynamic Topology

IoT networks are highly dynamic, with devices frequently joining and leaving the network. This mobility necessitates frequent key updates and redistributions, complicating the management process.

Resource Constraints

IoT devices are typically resource-constrained in terms of processing power, memory, and energy. Traditional cryptographic algorithms may be too demanding for these devices, necessitating lightweight solutions that still provide robust security.

Interoperability

The heterogeneity of IoT devices and communication protocols poses interoperability challenges. A key management scheme must be flexible enough to support various devices and standards while ensuring seamless integration.

Existing Key Management Approaches

Pre-Distributed Keys

In pre-distributed key schemes, keys are assigned to devices before deployment. While this method is straightforward and efficient for small, static networks, it is impractical for large-scale and dynamic IoT networks due to the need for frequent key updates.

Public Key Infrastructure (PKI)

PKI provides a scalable solution through asymmetric encryption but is computationally intensive and not suitable for resource-constrained IoT devices. Additionally, PKI requires a centralized authority, which can be a single point of failure.

Key Agreement Protocols

Key agreement protocols like Diffie-Hellman enable two devices to establish a shared secret over an insecure channel. While they are effective, these protocols tend to be too resource-intensive for IoT devices and do not scale well with dynamic topologies.

Proposed Framework for Secure and Efficient Key Management

Our proposed framework addresses the limitations of existing key management schemes by incorporating the following features:

Lightweight Cryptographic Algorithms
We utilize lightweight cryptographic algorithms specifically designed for IoT devices. These algorithms balance security and resource consumption, ensuring robust protection without overburdening device capabilities.

Dynamic Key Distribution

To handle the dynamic nature of IoT networks, our framework employs a dynamic key distribution mechanism. Keys are generated and distributed based on the current network topology and device status, minimizing the need for frequent rekeying.

Decentralized Architecture
A decentralized key management architecture eliminates the single point of failure associated with centralized systems. Distributed key authorities manage key distribution and updates, enhancing resilience and scalability.

Hierarchical Key Management
We implement a hierarchical key management scheme, where keys are structured in a multi-level hierarchy. This approach simplifies key distribution and updates, as changes at one level do not necessarily propagate throughout the entire network.

Security Analysis

Our framework provides robust security guarantees against common threats in IoT networks:

-Confidentiality: Lightweight encryption ensures that data is protected during transmission.
- Integrity: Hierarchical key management ensures that any tampering with data can be quickly detected and mitigated.
- Authentication: Dynamic key distribution and decentralized management ensure that only authorized devices can communicate within the network.

- Scalability: The hierarchical and decentralized architecture allows the system to scale efficiently, handling large numbers of devices without significant overhead.

Performance Evaluation

We carried out extensive simulations to assess the performance of our proposed framework. The results show that our approach significantly reduces both computational overhead and energy consumption compared to traditional key management schemes. Furthermore, our dynamic key distribution mechanism effectively adapts to changes in network topology, ensuring high levels of security while maintaining optimal performance..

Conclusion

Secure and efficient key management is critical for the success of IoT networks, especially given their dynamic and heterogeneous nature. Our proposed framework addresses the key challenges by integrating lightweight cryptographic algorithms, dynamic key distribution, and a decentralized, hierarchical architecture. This approach not only enhances security but also ensures scalability and resource efficiency, making it well-suited for large-scale IoT deployments.

References

1. D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586-615, 2003.
2. L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," in Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002, pp. 41-47.
3. A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, no. 5, pp. 521-534, 2002.
4. M. Bellare and P. Rogaway, "Entity Authentication and Key Distribution," in Advances in Cryptology - CRYPTO'93, 1993, pp. 232-249.
5. C. Karlof, N. Sastry, and D. Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks," in Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, 2004, pp. 162-175.
6. This paper presents a comprehensive framework for secure and efficient key management tailored to the unique challenges of dynamic IoT networks, paving the way for more resilient and scalable IoT deployments.