International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

A Comprehensive Survey of Identity-Based Key Management Techniques in Mobile Ad Hoc Networks (MANETs)

Kumar Amrendra[1*]

[1]Assistant Professor, Department of Computer Science Engineering and Information Technology, Jharkhand Rai University Ranchi, Jharkhand-834010, India

*Corresponding author e-mail: anshu.amrendra@gmail.com

Abstract

Cryptography forms a fundamental component of security mechanisms in mobile ad hoc networks (MANETs). Among various public key approaches, identity-based cryptographic techniques have gained significant attention for mobile environments because they simplify the key management process and reduce memory storage requirements. This paper presents an overview of existing identity-based key management schemes designed for MANETs. It also highlights several limitations and unresolved issues associated with these schemes, which remain insufficiently addressed and require further investigation in future research.

Keywords

Mobile Ad Hoc Networks, Identity based cryptography, Key Management

Introduction

A Mobile Ad Hoc Network (MANET) is a self-configuring and dynamic wireless network that enables communication among mobile nodes without relying on a centralized administration system. A MANET is composed of mobile platforms such as routers, wireless communication devices, and hosts, collectively referred to as nodes. These nodes can move freely and independently, leading to frequent changes in network topology.

The nodes in such networks may be deployed on various platforms including aircraft, ships, vehicles, or handheld devices carried by individuals. In many cases, a single router may serve multiple hosts. Nodes can join or leave the network at any time, which makes the structure of the network highly dynamic. Since routers move randomly and organize themselves autonomously, the wireless topology of the network may change rapidly and unpredictably. MANETs can operate independently or may be connected to the broader Internet infrastructure. Due to their minimal configuration requirements and rapid deployment capability, ad hoc networks are particularly useful in emergency situations such as natural disasters or other critical scenarios [7].

Overview of Key Management Schemes in Manet

Key management refers to the processes involved in establishing, distributing, and maintaining cryptographic keys among authorized entities in a network [9]. A keying relationship exists when two or more network nodes share cryptographic key material that enables secure communication. This key material may consist of a pair of public and private keys or secret keys used for encryption and decryption.

Achieving strong security in MANETs requires efficient key management mechanisms. However, managing cryptographic keys in such networks is challenging due to factors such as limited energy resources, lack of physical security, variable link capacities, and frequently changing network topology. Various cryptographic keys including symmetric keys, public keys, group keys, and hybrid keys (combining symmetric and asymmetric techniques) are employed for encryption in MANETs [8]. The following sections discuss some of the major key management techniques used in MANETs.

1. Symmetric Key Management in MANET

In symmetric key management, the same cryptographic key is used for both encryption and decryption of data. Both communicating nodes share a common secret key that must be kept confidential. Because a single key is used for both operations, symmetric encryption generally requires less computational power and is faster.

In contrast, public key cryptography employs two different keys: a private key and a public key. The private key is kept secret by the owner and is typically used for decryption, while the public key is openly available and used for encryption. A new pair of public and private keys can be generated for different communication sessions. Compared with symmetric systems, public key systems may require fewer shared keys between communicating nodes.

2. Asymmetric Key Management in MANET

Asymmetric key management utilizes two separate keys for encryption and decryption. Each node maintains a private key that is kept confidential and a public key that can be shared with other nodes. When a sender wants to transmit a secure message, it encrypts the data using the recipient's public key. The recipient then decrypts the message using their private key.

Since the private key is never shared or transmitted across the network, it remains secure from interception. This approach is commonly referred to as public key cryptography. Proper management of private keys enhances data protection and reduces the risk of information leakage.

3. Group Key Management Scheme in MANET

Group key management involves the use of a single cryptographic key shared among members of a group within the network. This key allows secure communication among all nodes that belong to the same group.

Group key management protocols are generally classified into three categories:

1. **Centralized schemes**, where a single controlling entity manages the creation, distribution, and updating of the group key.
2. **Distributed schemes**, where all participating nodes collaboratively generate and manage the group key.
3. **Decentralized schemes**, where multiple entities are responsible for generating, distributing, and updating the group key.

These approaches aim to ensure secure group communication while maintaining efficient key distribution among members.

4. Hybrid Key Management Schemes in MANET

Hybrid key management schemes combine two or more cryptographic techniques to enhance security and efficiency. Typically, these schemes integrate symmetric and asymmetric cryptographic methods. By combining the strengths of both approaches, hybrid schemes can provide efficient encryption while maintaining strong security for key distribution.

Identity-Based Cryptography

Identity-Based Cryptography (IBC) is a specialized form of public key cryptography in which a user's public key is derived directly from a unique identity, such as an email address, IP address, or node identifier. In this framework, a trusted entity known as the **Private Key Generator (PKG)** is responsible for generating the corresponding private keys for users.

The concept of IBC eliminates the need for traditional **Certificate Authorities (CA)** and **Public Key Certificates (PKCs)**. Several characteristics make identity-based cryptography particularly suitable for MANET environments [10]:

- It can be deployed without requiring extensive infrastructure, thereby avoiding the complexities of certificate distribution.
- It provides pairwise key establishment between nodes without requiring direct interaction.

- It requires relatively low computational resources, storage capacity, and communication bandwidth.
- The public key derived from the identity is self-authenticating and can contain useful information about the node.

The primary advantages of IBC include simplified key management and reduced memory requirements compared with conventional public key systems. It also enables easy deployment in environments where infrastructure support is limited.

Secure routing plays a critical role in MANETs, especially when sensitive data is transmitted between source and destination nodes. Without appropriate security mechanisms, routing information and transmitted data may be vulnerable to various attacks.

However, identity-based cryptography also has certain limitations. One significant issue is that the PKG must possess the private keys of all users in the network, which raises concerns about trust and security. In distributed MANET environments, assigning this responsibility to a single entity may create vulnerabilities. Additionally, identity-based systems often lack anonymity and privacy protection since public keys are directly derived from node identities.

Identity-Based Key Management

In an identity-based cryptographic system, a sender can encrypt a message using the receiver's identity as the public key. The receiver then decrypts the ciphertext using the private key generated by the PKG based on that identity.

A typical IBC framework consists of four main algorithms: **Setup, Extract, Encrypt, and Decrypt** [1].

- **Setup:** This algorithm takes security parameters as input and generates the master public key and master private key for the system. The master private key is maintained by the PKG.
- **Extract:** Using the master private key and a node's identity as input, this algorithm generates the private key for that particular node.
- **Encrypt:** This process uses the master public key, the sender's private key, the receiver's public key, and the message to produce encrypted ciphertext.
- **Decrypt:** Using the node's private key along with the master public key and ciphertext, the receiver decrypts the message to retrieve the original data.

The following subsections describe several important identity-based key management schemes developed for MANETs.

1. Khalili–Katz–Arbaugh Scheme

This scheme builds upon the Franklin and Boneh approach [2] and addresses certain limitations present in traditional key management methods that rely on Public Key Infrastructure (PKI) or shared secrets. The scheme integrates identity-based cryptography with threshold cryptography techniques. However, it does not provide mechanisms for key revocation or key renewal.

2. Deng–Mukherjee–Agrawal Scheme

This scheme incorporates two main components: distributed key generation and identity-based authentication [3]. The distributed key generation mechanism enables the creation of master public and private keys in a decentralized manner. The authentication component ensures secure end-to-end authentication between nodes within the network.

3. Bohio–Miri Scheme

This approach utilizes pairwise symmetric keys that are computed by nodes without interactive communication [4]. The scheme assumes that all nodes are properly initialized before the network is formed. During initialization, nodes receive public parameters and their respective private keys from the PKG. However, this requirement introduces dependence on external support structures and online servers, which somewhat contradicts the decentralized nature of identity-based systems.

4. Identity-Based Authentication and Key Exchange (IDAKE)

The IDAKE framework consists of two variants: **Basic MANET-IDAKE** and **Fully Self-Organized MANET-IDAKE** [5].

The basic MANET-IDAKE operates in two phases:

1. **Initialization Phase**, where nodes access an external PKG for setup, key extraction, and distribution.
2. **Operational Phase**, where nodes independently compute shared keys, manage key renewal, and perform key revocation without PKG involvement.

In the fully self-organized MANET-IDAKE model, all operations are handled directly by network nodes without requiring an external PKG. However, the scheme does not clearly define how private keys are initially distributed. The approach benefits from low bandwidth usage and reduced memory requirements due to efficient identity-based key management. While the basic model suffers from a single point of failure, the distributed variant eliminates this issue.

5. Identity-Based Key Management (IKM)

Identity-Based Key Management integrates identity-based cryptography with threshold cryptographic techniques [6]. In this approach, both public and private keys consist of two components: a node-specific identity-based element and a network-wide common element.

The node-specific component ensures that the security of uncompromised nodes remains intact even if some nodes are compromised. Meanwhile, the common component enables efficient network-wide updates of public and private keys through a single broadcast message.

Among the schemes discussed, most utilize asymmetric cryptographic keys, with the exception of the Bohio–Miri scheme, which employs symmetric key mechanisms.

Conclusion

This paper examined several identity-based key management schemes designed for mobile ad hoc networks. Identity-based cryptography represents a specialized form of public key cryptography that removes the need for certificate authorities and public key certificates, thereby simplifying key management.

Despite these advantages, identity-based approaches have certain limitations. One major concern is that the PKG must possess the private keys of all users in the system, which introduces potential security risks.

Future research may focus on developing improved methods that strengthen protection against various security threats in MANETs, including authentication, confidentiality, and data integrity.

References

[1] A. Khalili, J. Katz, and W.A. Arbaugh, “Towards Secure Key Distribution in Truly Ad-hoc Networks,” *Proc. SAINT Workshops, 2003, pp. 342-346.*

[2] D. Boneh and M. Franklin, “Identity based encryption from the weil pairing,” *Lecture Notes in Computer Science, vol.2139, pp. 213-229, 2001.*

[3] H. Deng, A. Mukherjee, and D.P. Agrawal, “Threshold and Identity Based Key Management and Authentication for Wireless Ad Hoc Networks,” *proc. Int’l Conf. Info. Tech.: Coding and Computing, vol.2, 2004, p. 107.*

[4] M. J. Bohio and A. Miri, “Efficient Identity Based Security Schemes for Ad Hoc Network Routing Protocols,” Ad Hoc
Networks, vol.2, no.3, 2004, pp.309-317.

[5] K. Hoeper and G. Gong, “Bootstrapping Security in Mobile Ad Hoc Networks Using Identity Based Schemes with Key
Revocation*,” tech. rep., Center for Applied Cryptographic Research, Univ. of Waterloo*, 2006.

[6] W. Liu, “Securing Mobile Ad Hoc Networks with Certificeteless Public Keys,” *IEEE Trans. Dependable Secure Computing*, vol.3, no. 4, 2006, pp.386-399.

[7] A. L.S. Orozeo, J.G. matesanz, L.J. G. Villalba, J. D. M. Diaz, and T. H. Kim, "Security issues in mobile ad hoc networks" *International Journal of distributed Sensor Networks, vol.2012, Dec 2012.*

[8] Merin Francis, M. Sangeetha, Dr. A. Sabari, "A Survey of Key Management Techniques for Secure and Reliable Data
Transmission in MANET," IJARCSSE, vol.3, issue 1, 2013, pp. 22-27.

[9] A. J. Menezes, P. C. V. *Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography*, CRC Press, 1996.

[10] S. Honarbakhsh, L. Latif, A. Manaf, B. Emami," Enhancing Security for Mobile Ad Hoc Networks by using Identity
Based Cryptography," IJCCE, vol. 3, no. 1, 2014.

[11] E. D. Silva and L. C. P. Albini, "Towards a fully-organized identity based key management system for MANETs," *IEEE 9th conf. on wireless and mobile computing, networking and communications,* 2013.

[12] "Cryptography and Network Security" by William Stallings, fifth edition.

[13] Amrendra, K., & Ranjan, P. (2020). Emerging trends and applications in mobile ad hoc networks (MANETs). *Advances in Science & Technology*, 10-18.