International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Enhancing MANET Performance through Effective Key Management: A Comprehensive Review

Dr. Gudelliwar Sandip S

Associate Professor
Aurora's PG College, Hyderabad

Abstract

A Mobile Ad-hoc Network (MANET) is a decentralized, infrastructure-less network with limited physical security and constrained resources, making robust security mechanisms essential. Key management plays a pivotal role in ensuring MANET security by handling key generation, storage, distribution, updating, revocation, deletion, and archiving. Key management protocols can be classified into four categories: symmetric, asymmetric, group, and hybrid. Among these, group key management has garnered significant research attention due to the growing prevalence of mobile devices and multicast communication. This paper comprehensively reviews various group key management strategies, evaluating them based on reliability, computational complexity, storage costs, communication overheads, prerequisites, security levels, robustness, vulnerabilities, scalability, energy efficiency, and mobility support. A comparative analysis is provided, highlighting the strengths and limitations of each protocol. The study concludes with an assessment of the trade-offs between different approaches, offering insights for future research directions.

Keywords*:* Data Mining, Cyber Security, Malicious Software, Intrusion Detection

Introduction

A Mobile Ad Hoc Network (MANET) is a self-configuring, infrastructure-less network where wireless mobile nodes collaborate to maintain connectivity, with each node functioning simultaneously as both a host and a router. Due to their rapid deployment, self-organizing capability, cost-effectiveness, and scalability, MANETs are highly sought after in various domains requiring decentralized wireless communication. These networks are widely employed in military operations, emergency response during natural disasters, healthcare systems, and other critical applications.

However, the absence of a fixed infrastructure, coupled with inherent challenges such as dynamic topology, limited bandwidth, node mobility, and short-lived connections, significantly compromises network security. The reliance on intermediate nodes for end-to-end communication exposes the network to potential attacks, where malicious actors may intercept, alter, or inject false data packets to disrupt communication integrity. These vulnerabilities underscore the need for robust security mechanisms to safeguard MANETs against exploitation.

The establishment of a group key enables multiple parties to derive a shared secret for secure communication. The Diffie-Hellman (DH) protocol allows two entities to generate such a secret without

relying on a trusted third party, and this approach can be extended to *n*-party scenarios through a generalized form of the two-party DH scheme. However, group key management must also address security challenges arising from dynamic membership changes. To maintain confidentiality, the group key must be refreshed—either periodically or immediately upon membership updates—to ensure both forward secrecy (new members cannot access past communications) and backward secrecy (departing members cannot access future exchanges).

Recent research has increasingly focused on optimizing group key update mechanisms, particularly in highly dynamic environments where frequent membership changes occur. With the growing adoption of collaborative and group-centric applications in MANETs, robust group key management has become a critical pillar of secure group communication. Nevertheless, designing scalable and secure group key management protocols for large, dynamic MANETs remains a significant challenge, as solutions must balance stringent security requirements with the inherent constraints of ad hoc networks, such as limited bandwidth, energy, and computational resources. “Two keys—one private and the other public—are used in public key cryptography. Encryption and decryption employ different keys. The source node stores the private key, which is only accessible to one person and is used for decryption. The public key, which is used for encryption, is accessible to everyone. New public and private key pairs are generated for each communication. Compared to symmetric key cryptography, it uses fewer keys. Short messages are sent using asymmetric keys, while longer messages are sent using symmetric keys. In a MANET, k keys are required for every n nodes that want to communicate, where k = 2n. In the field of cryptography, a group key is a single key that is exclusively given to one particular MANET group of mobile nodes. Creating and dispersing a secret for group members serves as the basis for generating a group key.” [1].

Three distinct types of group key protocol exist. 1. Centralized, in which a single entity controls and rekeys the group. 2. Distributed, group members or a mobile node that joins the group are equally liable for creating, dispersing, and rekeying the group keys. 3. The creation, distribution, and rekeying of the group key are decentralized; multiple organizations are in charge of doing so.

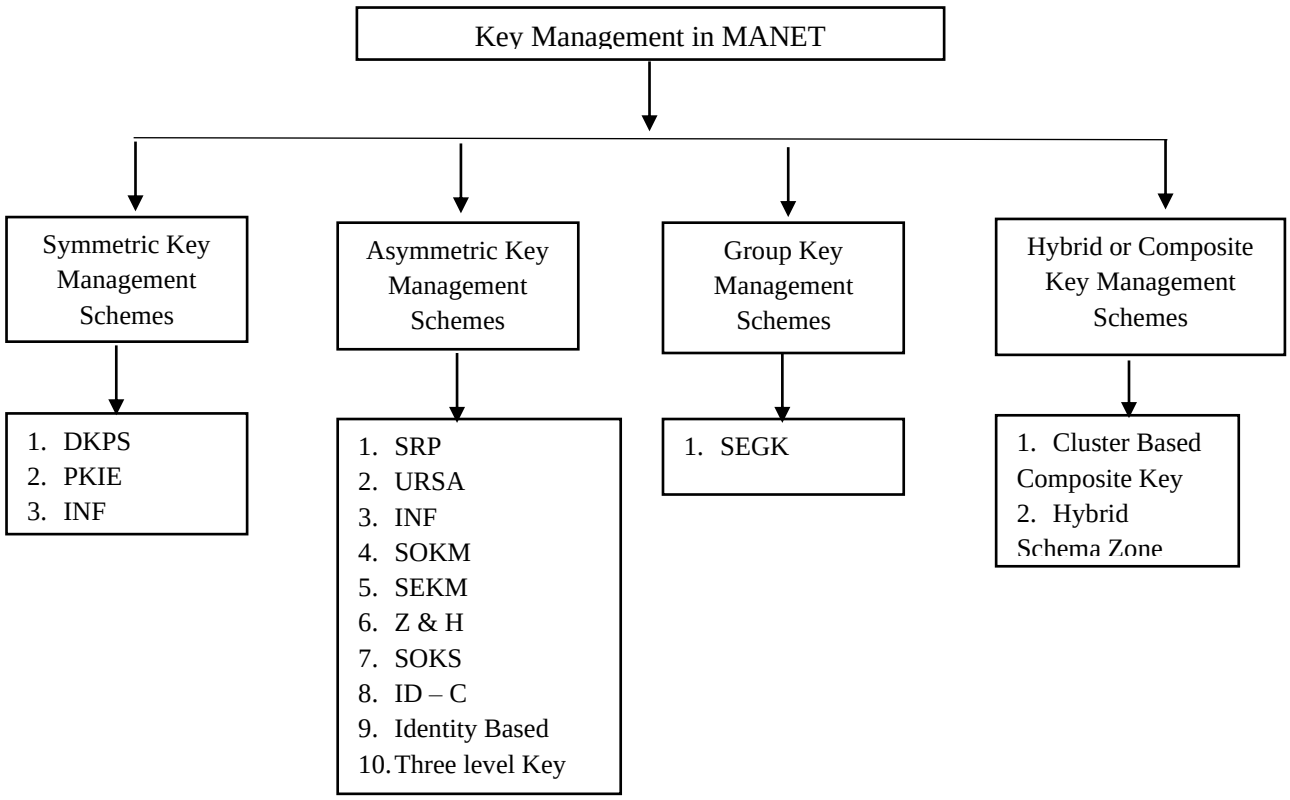

Fig. 1: Key Schemes in MANET

Key Management

Any network must have secure communication established. In comparison to their wired equivalents, the task is more difficult and complicated in mobile ad hoc networks. The usage of numerous little pieces of data known as keys is implied by the valuable instrument of cryptography, which is used to achieve this purpose. Key management systems must handle sensitive data safely since keys themselves are sensitive (KMS). When handling keys is necessary for secret communication between any two parties, including traditional and ad hoc networks should use a KMS. There are two primary categories of key usage. The first form, known as symmetric-key, occurs when every participant in the communication uses the same secret key, but the second type employs two separate keys for every participant. The asymmetric key is this kind. The public key is used for encryption, while the private key is utilized for decryption.

Various Key Management systems are employed in MANET to ensure the high level of security. Due to its energy-constrained operations, limited physical security, changeable capacity links, and dynamic topology, MANET places a high priority on using and managing keys for security.

Keys that are produced from the combination of two or more keys are known as hybrid or composite keys. These keys can be symmetric, asymmetric, or a combination of the two strategies for asymmetric key management Research publications have recently suggested various key management strategies for MANETs. The vast majority of them rely on public-key cryptography. The fundamental concept is to spread out the functionality of the CA among several nodes.

Robinson et al, (2016) suggested clustering with the key management system for routing in WSN. It assistance to resolve the difficulties met in a transmission of data security by presenting a simple key management mechanism, the secret sharing technology

Memon et al, (2017) suggested a novel technique to adjust the vehicle speed which decreases the vehicle delay experiences from network gap difficult. The writers recognized privacy-preserving authentication protocol to confirm vehicle activities in the terms of the privacy-preserving way.Wang et al, (2014) suggested a novel key management protocol for the strategic mobile scenario of MANETs. It commonly depends on the three proposed mechanisms to address the difficulty of improving energy-efficient security along with a performance of scalability for the protocol handling key establishment and distribution in the MANETs strategic mobile set-up.

Cho et al, (2016) researched about a new technique for managing the public key via soft securing mechanism founded on the notion of trust in MANETs.Masdari et al, (2017) explained the challenges in Wireless Body Area Network (WBAN) and its issues of key management. In this study, a comprehensive comparison and study of the key management capabilities in the proposed security and privacy schemes for the WBAN were offered.

T.V.Suresh Kumar et. Al. (2020) “concludes that CRA method is used for identifying the black hole node based on the information of nodes such as energy level and distance among the nodes. The detected black hole node’s information is saved in the routing table”.

Suresh R. Halhalli (2021) “presents an approach for trust-based secure routing protocol in MANET based on proposed AWOA. To enhance the security in routing protocol, the factors, like trust is considered as a major significant component. The trust mechanism is modelled by considering the trust factors, like AER, and SCF integrity factor and forwarding rate. Here, secure routing is carried out between the nodes using the proposed AWOA”.

Sending information to every other node inside the sending node's broadcast domain is referred to as broadcast communication. The entire network or a specific area of it known as the subnet may constitute the sender's broadcast domain. The most popular form of communication in MANETs is broadcasting because it can reach a lot of nodes. Nevertheless, numerous messages must be sent in order to reach a large number of destinations, which may not be wise in terms of network bandwidth. Prior to this, the routing protocols have solely employed broadcasts to share routing data. Due to this unintended resource consumption, nodes that are not meant to receive broadcast packets also have to process and forward the broadcast packets. Therefore, one of the most difficult problems in building a routing protocol for MANETs is minimising the amount of broadcasts.

Conclusion

This study examines recent advancements in group key management protocols for Mobile Ad Hoc Networks (MANETs). Using established evaluation criteria, we systematically assess and compare the three primary categories of group key management approaches: centralized, decentralized, and distributed architectures.

Our comparative analysis reveals that no single protocol demonstrates universal effectiveness across all MANET scenarios. Each approach exhibits distinct advantages and limitations when evaluated against critical parameters including computational efficiency, communication overhead, scalability, and

security robustness. The selection of an appropriate key management strategy must therefore consider specific application requirements and operational constraints.

The findings underscore the need for future research to develop adaptive key management solutions that optimally balance the fundamental trade-offs between security assurance, energy efficiency, and mobility support. Such solutions should particularly address the challenges posed by MANETs' dynamic topology and resource constraints while maintaining robust security guarantees.

REFERENCES

[1] JBing Wu, Jie Wu and YuhongDong,"An efficient group key management scheme for mobile ad hoc network", International Journal and Networks, Vol. 2008.

[2]. Robinson, Y. H., Balaji, S., & Rajaram, M. (2016). ECBK: Enhanced cluster based key management scheme for achieving quality of service. Circuits and Systems, 7(08), 2014.

[3]. Memon, I., Arain, Q. A., Memon, H., & Mangi, F. A. (2017). Efficient user based authentication protocol for location based services discovery over road networks. Wireless Personal Communications, 95(4), 3713-3732.

[4]. Wang, X., Yang, J., Li, Z., & Li, H. (2014). The energy-efficient group key management protocol for strategic mobile scenario of MANETs. EURASIP Journal on Wireless Communications and Networking, 2014(1), 161.

[5]. Cho, J. H., Chen, R., & Chan, K. S. (2016). Trust threshold based public key management in mobile ad hoc networks. Ad Hoc Networks, 44, 58-75.

[6]. Masdari, M., Ahmadzadeh, S., & Bidaki, M. (2017). Key Management in Wireless Body Area Network: Challenges and Issues. Journal of Network and Computer Applications.

[7]. T.V.Suresh Kumar, Dr.Prabhu G Benakop, 2020, "A Secure Routing Protocol for MANET using Neighbor Node Discovery and Multi Detection Routing Protocol", International Journal of Engineering Trends and Technology (IJETT) – Volume 68 Issue 7 - July 2020

[8]. Suresh R. Halhalli, 2021, "Optimisation driven-based secure routing in MANET using atom whale optimisation algorithm", Int. J. Communication Networks and Distributed Systems, Vol. 27, No. 1, 2021