International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-6)

Research Article

June 2015

Survey of Various Keys Management Techniques in MANET

Pratibha Kamboj
Mtech Student (CSE)
JMIT, Radur, Haryana, India

Nitin Goyal
Asst. Prof. (CSE)
JMIT, Radur, Haryana, India

Abstract-

Key management is a basic part of any secure communication structure. Secure communication protocol depends upon efficient key management technique. The key is a piece of input information for cryptography algorithms. Various key management schemes have been proposed in MANET. This paper describes various key management techniques in MANET. Based upon underlying cryptographic algorithm key management can be classified into symmetric and asymmetric. In symmetric key management same keys are used by sender and receiver. This key is used for encryption as well as for decryption of the data. In public key cryptography, two keys are used as private and public key. Different keys are used for encryption and decryption. The private key is available for individual, kept by source node and same is used for decryption also. To secure communications in Mobile Ad Hoc Networks (MANETs), messages are often protected by encryption using a chosen cryptographic key, which is the scenario of group communication called group key. Secure group communication systems typically rely on a group key, a secret shared by all members of the group. Privacy is provided by encrypting all data with the group key. The key management system controls access to the group key, ensuring that only authenticated members receive the key. Based upon trust level, group key management protocols can be classified into three categories namely, centralized, decentralized, and distributed. Another approach named hybrid key management has gained a lot of research attention. It combines various existing approaches to develop new technique.

Keywords— Group Key, Key management techniques, Mobile Ad Hoc Networks (MANETs), Cluster, Hybrid.

I. INTRODUCTION

A Mobile Ad-hoc network is a wireless ad-hoc network which is used to exchange information. Each node is willing to forward data to other nodes. It does not rely on fixed infrastructure. A node has straight connection with a set of nodes, said to be neighboring nodes, in an ad hoc network which are in its communication range. The number of nodes in the network is not fundamental preset. It has dynamic topology means links are formed and broken with mobility and has limited battery power.

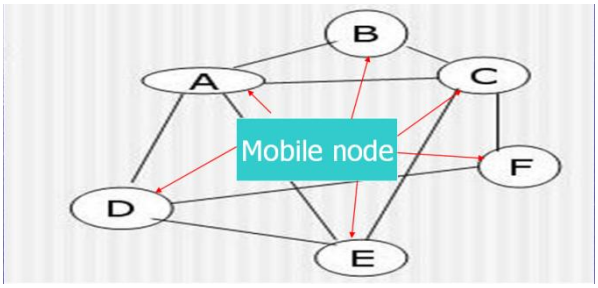

figure 1 Mobile Adhoc Network

There are many security issues in MANET like secure multicasting (where a single data packet can be transmitted from a sender and replicated to a set of receivers), secure routing, privacy-aware routing (building routing protocols that prevent intermediate nodes from performing traffic analysis) and key management.Key management is primary security issue because it is a central part of any secure communication. The main purpose of key management is to provide secure methods for handling cryptographic keying algorithm. The tasks of key management include keys for generation, distribution and maintenance. Key maintenance includes the procedures for key storage, key update, and key revocation. Different cryptographic keys are used for encryption like symmetric key, asymmetric key, hybrid key (symmetric key + asymmetric key) and group key [1]. In symmetric key management same keys are used by sender and receiver. This key is used for encrypting the data as well as for decrypting the data. Asymmetric keys uses two-part key. Each recipient has a private key that is kept secret and a public key that is published for everyone. The sender looks up or is sent the recipient's public key and uses it to encrypt the message. The recipient uses the private key to decrypt the message and never publishes or transmits the private key to anyone. Thus, the private key is never in transit and remains invulnerable. This system is sometimes referred to as using public keys. This reduces the risk of data loss and increases compliance management when the private keys are properly managed.

Group key in cryptography is a single key which is assigned only for one group of mobile nodes in MANET. For establishing a group key, group key is creating and distributing a secret for group members. There are specifically three categories of group key protocol

1. Centralized, in which the controlling and rekeying of group is being done by one entity.
2. Distributed, group members or a mobile node which comes in group are equally responsible for making the group key, distribute the group key and also for rekeying the group.
3. Decentralized, more than one entity is responsible for making, distributing and rekeying the group key.

While centralized approaches are of least interest in MANETs, decentralized approaches have gained a lot of research attention. The fully distributed trust model is also favored for MANETs. Interestingly, a hybrid approach that combines the centralized model with the distributed scheme has been proposed recently [2].

Cluster based approach can also be used to achieve group communication. Cluster is eventually said to be group, while clustering is a phenomenon of collecting sub groups. Local controller (LC) is used to manage each sub-group, liable for local key management within its own cluster. Cluster head generates group key which communicate to other members through a secure and constrained channel that uses public key cryptography. Bechler et al. in [4] proposed cluster-based security architecture for Ad hoc networks. A network is divided into clusters with one unique head node for each cluster. These cluster head nodes carry out organizational functions and shares a network key among other members of the cluster. Moreover the same key is used for certification. In each cluster, exactly one distinguished node–the cluster head (CH)–is responsible for establishing and organizing the cluster.

The rest of this paper is structured as follows. Section II describes some key management techniques and section III describes conclusion.

II. RELATED WORK

Key management is a very important part of any safe communication. Most cryptosystems rely on some necessary secure, robust, and efficient key management system. This section discusses some of the related proposed key management schemes for secure group communication in wireless ad hoc networks. Maghmoumi et al. in [6] proposed a cluster based scalable key management protocol for ad hoc networks. Their proposed protocol is related to a new clustering technique. The network is segregated into communities or clusters based on similarity relationships between nodes. In order to make sure the trusted communications between nodes they proposed two types of keys generated by each cluster head. The protocol is adaptive according to the restriction of the mobile nodes battery power and to the dynamic network topology changes. This proposed approach of clustering is based scalable key management protocol provided protected communications between the nodes of the ad hoc networks. A key management proposal for secure group communication in MANETs was described by Wang et al. in [7]. They illustrate a hierarchical key management scheme (HKMS) for secure group communications in MANETs. For the sake of security, they encrypted a packet twice. They also converse about group maintenance in their paper in order to deal with changes in the topology of a MANET. At last, they carried out a performance analysis to compare their proposed scheme with other conventional methods that are used for key management in MANETs. The results demonstrate that their proposed method performed well in providing secure group communication in MANETs.

A new group key management protocol for wireless communication ad hoc networks was stated by Rony et al. in [9]. They put forth a well-organized group key distribution (most commonly known as group key agreement) protocol which is based on multi-party Diffie Hellman group key exchange and which is also password authenticated. The basic idea of the protocol is to securely construct and distribute a secret session key, 'K,' among a group of nodes/users who want to communicate among themselves in a secure manner. The projected protocol starts by constructing a spanning tree on-the-fly concerning all the valid nodes in the scenario. It is understood, like all other protocols that each node is individually addressed and knows all its neighbors. The password 'P' is also most common among each valid member present in the scenario. This 'P' helps for authentication process and prevents man in-the-middle attack. Unlike several other protocols, the proposed approach does not need broadcast/multicast capability.

Bechler et al. in [10] proposed cluster-based security architecture for Ad hoc networks. They proposed security concept based on a distributed certification facility. A network is divided into clusters with one unique head node for each cluster. These cluster head nodes carry out organizational functions and shares a network key among other members of the cluster. Moreover the same key is used for certification. In each cluster, exactly one distinguished node–the cluster head (CH)–is responsible for establishing and organizing the cluster. Clustering is also used in some of the routing protocols for ad hoc networks. Decentralization is attained using threshold cryptography and a network secret that is distributed over a number of nodes. A scalable key management and clustering scheme was anticipated by Jason et al. in [12]. They estimated a scalable key management and clustering scheme for secure group communications in ad hoc networks. The scalability problem is solved by segregating the communicating devices into subgroups, with a leader in each subgroup, and further organizing the subgroups into hierarchies. Each level of the hierarchy is called a tier or layer. The hierarchical flow is in order of Key generation, distribution, and actual data transmissions. Distributed Efficient Clustering Approach (DECA) present a robust clustering to form subgroups, and analytical and simulation results demonstrate that DECA is energy-efficient and resilient against node mobility. Match up to other schemes, their approach is extremely scalable and efficient, provides more security guarantees, and is selective, adaptive and robust.

Vimala et al. in [3] proposed a Simple and Efficient Group Key (SERGK) management scheme for Region based MANET. The basic idea of SERGK is that a physical multicast tree is formed in MANETs for efficiency. Group members take turns acting as group coordinator to compute and distribute intermediate key materials to group members. The keying materials are delivered through the tree links. The coordinator is also responsible for maintaining the connection of the multicast group. All group members can calculate the group key locally in a distributed manner. This approach has reduced the computation cost and time and provides better scalability than cluster based approach.

Most existing security mechanisms for MANETs thus far involve the heavy use of public-key certificates. Yanchao Zhang et al. in [5] presented an ID-based key management scheme as a novel combination of ID-based and threshold cryptography. IKM is a certificateless solution in that public keys of mobile nodes are directly derivable from their known IDs plus some common information. It thus eliminates the need for certificate based authenticated public-key distribution indispensable in conventional public-key management schemes. Jin-Hee Cho et al. in [8] proposed a fully distributed trust-based public key management approach for MANETs using a soft security mechanism based on the concept of trust. They proposed a composite trust-based public key management (CTPKM) with no centralized trust entity with the goal of maximizing performance (e.g., service availability or efficiency) while justifying security vulnerability. Each node employs a trust threshold to determine whether or not to trust another node. Each node's decision making using the given trust threshold affects performance and security of CTPKM.

III. CONCLUSION

MANET is one where there is no programmed infrastructure such as base stations or mobile switching centers. Key management in the ad hoc network is a difficult issue concerning the security of the group communication. In Mobile ad hoc networks (MANETs) security has become a primary requirements .The characteristics capabilities of MANETs expose both challenges and opportunities in achieving key security goals, such as confidentiality, access control, authentication, availability, integrity, and non- repudiation. Most cryptographic mechanisms, such as symmetric and asymmetric cryptography, often involve the use of cryptographic keys. However, all cryptographic techniques will be unsecure or inefficient if the key management is weak. Key management is also a central component in MANET security. The main purpose of key management is to provide secure methods for handling cryptographic keying algorithm. The tasks of key management include keys for generation, distribution and maintenance. Key maintenance includes the procedures for key storage, key update, key revocation, etc. In MANETs, the computational load and complexity for key management are strongly subject to restriction by the node's available resources and the dynamic nature of network topology. An efficient technique for key management in MANET's can be developed using a hybrid key management approach makes use of both symmetric and asymmetric techniques in an attempt to exploit the advantages of both techniques and which does not require certification authority.

REFERENCES

[1] Merin Francis, M. Sangeetha and Dr. A. Sabari, "A Survey of Key Management Technique for Secure and Reliable Data Transmission in MANET", "International Journal of Advanced Research in Computer Science and Software Engineering", pp. 22-27 January – 2013.

[2] Abu Taha Zamani and Syed Zubair, "Secure and Efficient Key Management Scheme in MANETs", IOSR Journal of Computer Engineering (IOSR-JCE), vol. 16, no. 2, pp. 146-158, 2014.

[3] N. Vimala, B. Jayara and Dr. R. Balasubramanian, "Efficient Group Key Management Protocol for Region Based MANETs", IACSIT International Journal of Engineering and Technology, Vol.3, no.1, pp. 1793-8236, February 2011.

[4] Mohamed-Salah Bouassida, Isabelle Chrisment, and Olivier Festor, "Group Key Management in MANETs," International Journal of Network Security, vol. 6, no. 1, pp. 67-79, 2008.

[5] Yanchao Zhang ,Wei Liu, Wenjing Lou, and Yuguang Fang, "Securing Mobile Ad Hoc Networks with Certificateless Public Keys",IEEE Transactions on Dependable and Secure Computing, vol. 3,no. 4, October-December 2006.

[6] Chadi Maghmoumi, Hafid Abouaissa, Jaafar Gaber, and Pascal Lorenz, "A Clustering-Based Scalable Key Management Protocol for Ad Hoc Networks," Second International Conference on Communication Theory, Reliability, and Quality of Service, pp.42-45, 2009.

[7] Nen-Chung Wang, and Shian-Zhang Fang, "A hierarchical key management scheme for secure group communications in mobile ad hoc networks," Journal of Systems and Software, vol. 80, no. 10, pp. 1667-1677, 2007.

[8] Jin-Hee Cho, Kevin S. Chan and Ing-Ray Chen, "Composite Trust-based Public Key Management in Mobile Ad Hoc Networks".

[9] Rony H. Rahman, and Lutfar Rahman, "A New Group Key Management Protocol for Wireless Ad-Hoc Networks," International Journal of Computer and Information Science and Engineering, vol. 2, no. 2, pp. 74-79, 2008.

[10] M. Bechler, H. -J. Hof, D. Kraft, F. Pählke, and L. Wolf, "A Cluster- Based Security Architecture for Ad Hoc Networks," Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM, vol. 4, pp. 2393-2403, 2004.

[11] Yi Jim Chen, Yi Ling Wang, Xian Ping Wu, and Phu Dung Le, "The Design of Cluster-based Group Key Management System in Wireless Networks," pp. 1-4, 2006.

[12] Jason H. Li, Renato Levy, Miao Yu, and Bobby Bhattacharjee, "A scalable key management and clustering scheme for ad hoc networks," Proceedings of the 1st international conference on Scalable information systems, 2006.

