Volume 3, Issue 1, January 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey of Key Management Technique for Secure and Reliable Data Transmission in MANET

Merin Francis[*]
M.Tech (IT)
Dept of Information Technology
K.S.R College of Technology,
Tiruchengode, India

M. Sangeetha
Assistant Professor
Dept of Information Technology
K.S.R College of Technology,
Tiruchengode, India

Dr. A. Sabari
Professor
Dept of Information Technology
K.S.R College of Technology,
Tiruchengode, India

Abstract - A Mobile Ad-Hoc Network (MANET) is a self-configuring network of mobile nodes connected by wireless links to form an arbitrary topology without the use of existing infrastructure. Due to the nature of Unreliable Wireless medium Data Transfer is a major Problem in MANET and it lacks Security and Reliability of Data. Cryptographic techniques are commonly used for secure Data transmission wireless networks. Most cryptographic techniques, such as symmetric and asymmetric cryptography, often involve the use of cryptographic keys. However, all cryptographic techniques will be useless if the key management is weak. Key management is the central component in MANET security. There are number of key management schemes have been proposed for MANET. In this survey, we present a complete analysis of various key management techniques to find an efficient key management for Secure and Reliable Data transmission in MANET.

Keywords - MANET, SEGK, PGSK, PIKE, INF, DKPS, SOKM, SEKM, Symmetric Key, Asymmetric Key.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring network of mobile nodes connected by wireless links, to form an arbitrary topology. The nodes are free to move randomly. Thus the network's wireless topology may be unpredictable and may change rapidly. Minimal configuration, quick deployment and absence of a central governing authority make ad hoc networks suitable for emergency situations like natural disasters, military conflicts, emergency medical situations etc. [1] [2].

Secure communication [3], an important aspect of any networking environment, is an especially significant challenge in ad hoc networks. The unreliable wireless medium in MANET is a threat for Secure Data Transmission. The communication in mobile ad hoc networks comprises two phases, the route discovery and the data transmission. In an adverse environment, both Phases are vulnerable to a variety of attacks, one way to counter security attacks would be to cryptographically protect and authenticate all control and data traffic. Key management [4] is a basic part of any secure communication structure. Most secure communication protocols rely on a secure, robust, and efficient key management system. The key is a piece of input information for cryptography algorithms.

Different cryptographic keys [5] are used for encryption like symmetric key, public key, group key and hybrid key (symmetric key + asymmetric key). In symmetric key management same keys are used by sender and receiver. This key is used for encryption the data as well as for decryption the data. In public key cryptography, two keys are used one private key and another public key. Different keys are used for encryption and decryption. The private key is available only for individual and kept by source node and it is used for decryption.

In MANET there are various Key Management Schemes proposed. To secure communications in Mobile Ad Hoc Networks (MANETs), messages are often protected by encryption using a chosen cryptographic key, which, in the scenario of group communication is called the group key proposed in [6]. Multicast [7] is a communication service that provides data delivery from a source to a set of recipients, also known as multicast group. 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.

A new peer-to-peer key management scheme called, Self-organized Peer-to-Peer Key Management (SelfOrgPKM), is proposed in [8]. SelfOrgPKM is specifically designed for fully self-organized MANETs, i.e. MANETs that do not rely on any form of trusted authority. As building blocks for SelfOrgPKM the notion of subordinate public keys and a variant on the ElGamal signature scheme is presented. These building blocks may find application in various other security schemes. Other than that ID based key, Cluster based Key, Mobility based Key, Parallel Key, are discussed in [8]. In our Survey we have analysed various Key Management schemes to find an Key Management scheme that meets the necessary parameter of Reliable and Secure data transmission in MANET.

II. OVERVIEW OF KEY MANAGEMENT SCHEMES IN MANET

A keying relationship is the state wherein network nodes share keying material for use in cryptographic mechanisms. The keying material can include public/private key pairs, secret keys, initialization parameters and non-secret parameters supporting key management in various instances. Key management can be defined as a set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties. Fig. 1 shows the different existing key management schemes for MANET.

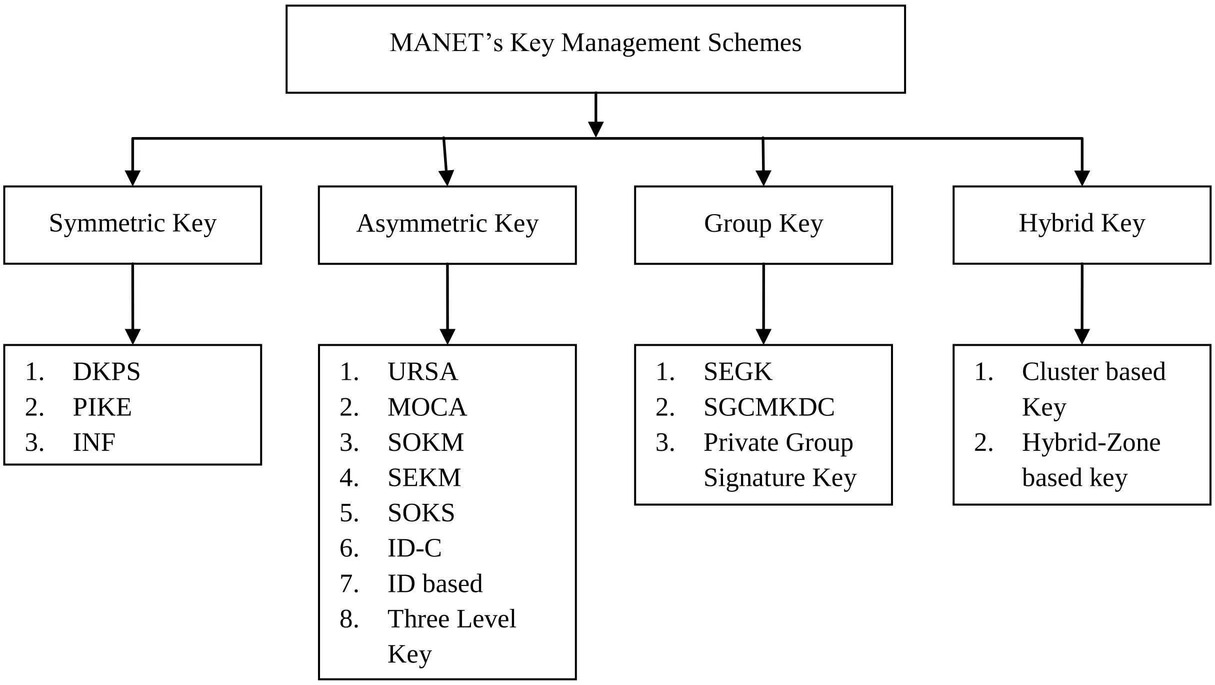

Fig. 1 Key Management Schemes in Mobile adhoc Networks

To achieve the high security in MANET different Key Management schemes are used. Using and managing keys for security is a crucial task in MANET due its energy constrained operations, limited physical security, variable capacity links and dynamic topology Different cryptographic keys are used for encryption like symmetric key, public key, group key and hybrid key (symmetric key + asymmetric key). Let us discuss about some of the important Key Management techniques in MANET.

A. Symmetric Key Management in MANET

In symmetric key management same keys are used by sender and receiver. This key is used for encryption the data as well as for decryption the data. If n nodes wants to communicate in MANET k number of keys are required, where k = n (n-1)/2. In public key cryptography, two keys are used one private key and another public key. Different keys are used for encryption and decryption. The private key is available only for individual and kept by source node and it is used for decryption. The public key is used for encryption and it available to the public. In each communication new pair of public and private key is created. It requires less no of keys as compared to symmetric key cryptography. Let us discuss about some of the symmetric key management schemes in MANET.

Distributed Key – Pre Distribution Scheme (DKPS):

DKPS basically consist of three important phases 1. Distributed Key Selection (DKS) In the first phase every node takes the

Random key from the universal set by using exclusion property. 2. Secure Shared-key Discovery (SSD): This is second phase of DKPS in which every node having a shared key with another node. Node can't found that which key in the ring are in common with which node. The trivial method is used for SSD. This method is not providing security but easy to evaluate because eavesdropping can occur in DKS phase.3. Key Exclusion Property Testing (KEPT) Last phase of DKPS symmetric key management scheme is KEPT. Incidence matrix is used for present the relationship between mobile nodes key and shared keys it using binary values for constructing the matrix. DKPS needs less storage as compared to pair-wise key agreement approach. This scheme is more efficient as compared to group key agreement [9].

Peer Intermediaries for Key Establishment (PIKE):

This model uses the senor nodes to establish the shared key. PKIE is symmetric key agreement scheme, it using unique secret key in a set of nodes .This model is using the concept of random key pre-distribution, and in 2-D case with each of the O (n) nodes every mobile node shares a unique secret key in horizontal and vertical dimension. This scheme can be extended to 3D or any other dimension. In MANET, every pair of mobile node shares a common secret key with at least 1 or more intermediaries. Features of this model are good security services, and fair scalability [10].

Key Infection (INF):

This model is simple and every mobile node participates equally to making the key establishment process. INF model having no need of collaborative effort because node acts as a trust component, this component broadcast their symmetric key. This model having weak security services but INF having low storage cost, low encryption, and low operation. It is having fair scalability with the problem of late entry of mobile node. Good resources efficient survivability in this model with low intermediaries [11].

B. Asymmetric Key Management Scheme in MANET

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. Let us discuss some important asymmetric key management schemes in MANET.

Self-Organized Key Management (SOKM):

SOKM model using two local certificate repositories one is updated and another one is non updated certificate repository. For calculating the best certificate graph each node maintains the non-updated certificate repositories. Every mobile node generates public key certificate to other mobile nodes and each mobile node act as their own authority. Public key chain certificate is using for doing the key authentication process. SOKM have great configuration flexibility and no need of boot strapping process. Web-of-trust relationship is used for certificate path and it is not strongly connected which is not suitable for ad-hoc network [12].

Secure and Efficient Key Management (SEKM):

This is only one decentralized asymmetric key management scheme (based upon virtual CA trust model) which provides detailed, safe procedure for interacting, coordination between secret shareholders, and efficient that have more responsibility. This model uses mesh structure for server group. This server group consisted with all servers which having the partial system private key that use to connect the server group. To providing certificate services, maintain the connection of the group and for share updates SEKM using periodic beacons. The cost of maintaining the structure server group is high [13].

Private ID based Key Asymmetric Key Management Scheme:

Without using the environment of PKI Secure Identity-Based Key management scheme is proposed in [14]. This scheme consisted with four phases. To verify the user identity and generating the corresponding private keys this scheme needs trusted key generation centre. RSA scheme is used to construct the private-public key pair; each mobile node in MANET gets his long term public and private key pair. The secret key as a master key is chosen by key generation centre randomly as well as publish its corresponding public key. After the security analysis of this model, it provides end-to-end authenticity and it prevents the network from brute force attack, man in a middle attack and from replay attack. Mobile nodes have no need to producing their public key and to broadcast the keys in the network.

C. Group Key Management Scheme in MANET

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. Let us discuss about some important Group key Management schemes in MANET.

Simple and Efficient Group Key Management (SEGK):

In SEGK two multicast tree are constructed in MANET for improving the efficiency and maintains it in a parallel fashion to achieve the fault tolerances. SEGK model calls one multicast tree as a blue tree and another multicast tree as a red tree. The connection of multicast tree is maintained by coordinator. Computation and distribution of intermediates keying materials to all member is does by group coordinator through the use of underlying tree links. To makes the common group key each group member i.e. mobile node in MANET, participates in a share of a final common group key, which is updated periodically. This model presents the reliable double multicast tree formation and maintenance protocol, which ensures that it covers all group members. The initialization process is start by group coordinator with sending the join advertise message into the mobile ad-hoc network. No of mobile nodes are directly propositional to computation cost. In SEGK model, any mobile node or group member can join and leave the network. To ensure the backward and forward security updating of group key is done very frequently. Two detection methods are described in SEGK model, (a) Tree Links, when the node mobility is not significant detection is done through tree links. (b) Periodic Flooding of Control Messages, for high mobility environment this method is used [6].

Private Group Signature Key (PGSK):

Group signatures are proposed in [15], provide anonymity for signers. Any member of the group can sign messages, but the resulting signature keeps the identity of the signer secret. In some systems there is a third party that can trace the signature, or undo its anonymity, using a special trapdoor. Some systems support revocation where group membership can be selectively disabled without affecting the signing ability of unrevoked members. Currently, the most efficient constructions are based on the Strong-RSA assumption. A Private Group Signature key is generated by a Key Server for each node in the Network which ensures full anonymity which means a signature does not reveal the signer’s identity but everyone can verify its validity.

D. Hybrid Key Management Schemes in MANET

Hybrid or composite keys are those key which are made from the combination of two or more than two keys and it may be symmetric or a asymmetric or the combination of symmetric & asymmetric key. Let us discuss about some of the important Hybrid key management schemes in MANET.

Cluster Based Composite Key Management:

This scheme takes the concept of off-line CA, mobile agent, hierarchical clustering and partial distributes key management. Public key of the members are maintained by cluster head that reduces the problem of storage in PKI. Mobile agents provide node revocation and PKG services in MANET. On the basis of current trust value and old public key, cluster head’s public key is computed. Using the timestamp in key number key renewal process can be done easily. MA handles the role of key revocation process and the selection of PKG nodes. It supports network extendibility through hierarchical clustering. This model saves network bandwidth and storage space [16].

Zone-Based Key Management Scheme:

This scheme uses ZRP (Zone Routing Protocol) proposed in [17], in this model for each mobile node zone is defined. Some pre-defined number is allocated to each mobile node which depends on the distance in hops. Symmetric key management is used by mobile node only for intra or inside r zone (zone radius). Without depends on clustering mobile node uses asymmetric key management for inter-zone security. It provides efficient way to making the public key without losing the capability of making the certificates.

III. COMPARATIVE SURVEY

In the Previous Section we have discussed about some of the most important Key Management Techniques in Mobile adhoc networks. In Comparative survey we are going to compare these Key Management techniques based upon some of the Features like Reliability, Security, Scalability and Robustness. The Comparative Survey is made depending upon the results that are analysed from various research works and journals. Table I shows the Comparative Survey of Key Management schemes in Mobile adhoc Networks. Let us discuss about the features of Key Management schemes that we are going to compare.

Reliability:

The Reliability of a Key Management scheme depends upon the Key Distribution, Storage and Maintenance. It is necessary to make sure that the Keys are Properly Distributed among the nodes, safely stored where intruders aren’t able to hack the keys and should be Properly Maintained.

Scalability:

Key management operations should finish in a timely manner despite a varying number of nodes and node densities. The fraction of the available bandwidth occupied by network management traffic should be kept as low as possible. Any increase in management traffic reduces available bandwidth for payload data accordingly. Hence, scalability of key-management protocols is crucial.

Security:

Authentication and intrusion tolerance is a primary concern to ensure no unauthorized node receives key material that can later be used to prove status as a legitimate member of the network. Nobody should provide private keys or issue certificates for others unless the others have been authenticated. Intrusion tolerance means system security should not succumb to a single, or a few, compromised nodes. Other central security issues are trust management and vulnerability. Trust relations may change during network lifetime. The system should enable exclusion of compromised nodes. In order to judge the security of a key-management scheme, possible vulnerabilities should be pinpointed. Proper key lengths and cryptographic algorithms of adequate strength are assumed.

Robustness:

The key-management system should survive despite denial-off service attacks and unavailable nodes. The key-management

operations should be able to be completed despite faulty nodes and nodes exhibiting byzantine behaviour, that is, nodes that deliberately deviate from the protocol. Necessary key management operations caused by dynamic group changes should execute in a timely manner. Key management operations should not require network wide and strict synchronization.

TABLE I
Comparative Survey of Key Management Schemes

	Reliability	**Security**	**Scalability**	**Robustness**
DKPS	Medium	Fair	Fair	Good
PIKE	Medium	Limited	Fair	Fair
INF	Low	Poor	Good	Good
SOKM	Medium	Fair	Fair	Good
SEKM	High	Good	Fair	Good
Private ID based Key	High	Good	Good	Fair
SEGK	Low	Poor	Good	Good
PGSK	High	Good	Fair	Good
Cluster based Key	Medium	Limited	Fair	Limited
Zone based Key	Low	Limited	Poor	Fair

The Reliability is rated by High, Medium and Low. While Security, Robustness and Scalability are rated by Good, Fair, Poor and Limited. Where Limited states the undependable nature of that particular feature.

IV. CONCLUSION

This Paper we have surveyed the key management schemes for Mobile adhoc networks. We gave a brief description about all the key management schemes discussed above and then a comparative survey has been made depending upon the characteristics and the features of the key management schemes. The comparative survey is carried out for the key management schemes based upon the features like Reliability, Scalability, Robustness and Security. The Analysis gave a interesting result where the Private ID based Key and Private Group Signature key Schemes performs well for Mobile adhoc networks.

REFERENCES

[1] S. Corson and J. Macker, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, RFC: 2501, Jan 1999.

[2] Carlo Kopp, “Ad Hoc Networking”, Systems Journal, pp 33-40, 1999.

[3] A Review on Key Management Schemes in MANET - Renu Dalal1#,Yudhvir Singh2 and Manju Khar International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012.

[4] Secure message transmission in mobile ad hoc networks - Panagiotis Papadimitratos *, Zygmunt J. Haas.

[5] Anne marie hegland, eliwinjum, stig f. Mjølsnes, chunming rong, Øivind kure, and pål spilling “A Survey of Key Management in Ad hoc networks” ieee 3rd quarter 2006, volume 8, no. 3

[6] Bing Wu, Jie Wu, Yuhong Dong “An efficient group key management scheme for mobile ad hoc networks” Int. J. Security and Networks. Vol. 2008.

[7] V. Palanisamy, P. Annadurai “Secure Group Communication using Multicast Key Distribution Scheme in Ad hoc Network” 2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 25.

[8] Johann van der Merwe, “Key Management in Mobile Ad Hoc Networks”.

[9] Aldar C-F. Chan, “Distributed Symmetric Key Management for Mobile Ad hoc Networks”, IEEE, 2004.

[10] Aziz, B., Nourdine, E. and Mohamed, E., “A Recent Survey on Key management Schemes in MANET”ICTTA’08, pp. 1-6, 2008.

[11] R. Anderson, Haowen and Perring, Adrian, “Key Infection: Smart trust for smart dust”, 12th IEEE International Conference on Network Protocol ICNP, 2004.

[12] Valle, G. and Cerdenas, R., “Overview the key Management in Ad Hoc Networks”, ISSADS pp. 397 – 406, 2005.

[13] Wu, B., Wu, J., Fernandez, E., Ilyas, M. and Magliveras, S., “Secure and Efficient key Management in mobile ad hoc networks”, Network and Computer Applications, Vol. 30, pp. 937-954, 2007.

[14] AnilKapil and SanjeevRana, “Identity-Based Key Management in MANETs using Public Key Cryptography”, International journal of Security, vol. (3): Issue (1).

[15] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in Advances in Cryptology–Crypto’04, Lecture Notes in Computer Science, vol. 3152, 2004, pp. 41–55.

[16] R. PushpaLakshmi, A. Vincent Antony Kumar,"Cluster Based Composite Key Management in Mobile Ad Hoc Networks", International Journal of Computer Applications, vol. 4- No. 7, 2010.

[17] ThairKhdour, Abdullah Aref, "A HYBRID SCHEMA ZONE-BASED KEY MANAGEMENT FOR MANETS", Journal of Theoritical and Applied Information Tecnology, vol. 35 No. 2, 2012.