International Journal of Computer Science and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 5, Issue 2, Feb - Mar 2016, 81-90

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

COMPREHENSIVE STUDY ON KEY MANAGEMENT SCHEMES IN MANET

NAMAN VAISHNAV[1] & HARDIK UPADHYAY[2]

[1]Research Scholar, GTU PG School, Ahmadabad, India

[2]Assistant Professor, GPERI, Mehsana, India

ABSTRACT

MANET does not have pre-existing fixed structure. Mobile nodes send packets to the destination nodes directly or via the intermediate nodes. Nodes exchange packets with each other to allow the message to pass among both ends step by step. These packets are outside the wireless transmission range. It is for potential security concern because intermediate nodes cannot be trusted. With such feature ad-hoc networks are least attacked which influences performance of the network with its reliability. Secure communication in MANET is to be claimed by the reliability parameter of the key management strategy, which is capable for securing contents among the nodes. This survey presents the conceptual view for various key management techniques with their special features.

KEYWORDS: Manet, Symmetric Key, Hybrid Key Cryptography, Group Key, Asymmetric Key, Key Management

I. INTRODUCTION

In MANET mobile nodes sends packets to the destination nodes directly or via neighboring nodes, it is potentially a security concern because neighbor nodes cannot be trusted. MANET does not have any pre-existing structure. However, MANET protocols are vulnerable to different type of security attacks. Furthermore, mobile nodes commonly function on the battery power it means all modules should be optimized to provide extended battery lifetime. (Moreover, malicious nodes may inject bogus data into the network to consume its scare resources, and selfish nodes can drop data packets of other nodes). From the security point of view, services of centralized network may consist a focused attack in which a single node is responsible for the network's security whereas, decentralized network functionally keeps away this kind of focused attacks. To achieve CIA-Trio in decentralized networks, mainly two mechanism are there which are Trust based and Cryptography. From that a cryptography is most efficient technique to achieve security. To ensure this parameters in MANET environment the problem of key management arises. Key management can be considered as the set of important techniques and processes attached with establishment and improvisation of key relationships between the entities. Keying relationship is process in which various nodes starts sharing keying subject that can be public or private keys. In short, key management processes are the cause of key agreement as well as key transport. Different cryptographic keys are used to encrypt important data in MANETs. Symmetric key, asymmetric or public key, hybrid key (symmetric key + asymmetric key) and group key are the types of various cryptographic keys. This paper will give the overview of current key management schemes required for the MANETs. Schemes are sectioned based on the type of key used. This paper provides brief description of the available key management schemes for MANETs.

This paper is divided into five sections. Section II describes vulnerabilities in MANETs. Section III explains symmetric key management strategy while section IV introduces asymmetric key management strategy. Section V and VI presents group and hybrid key management strategies for MANETs respectively [25, 26].

II. VULNERABILITIES IN MANET

MANET is a group in which mobile nodes are moving arbitrarily. So that the networks topology changes frequently and as a result the trust among the nodes creates complications in routing data. The security of the Mantes begins with the investigation and identifying of vulnerability in the system and the process of data exchange in the network. To obtain acceptable level of security in routing protocol which helps to protect the environment from malicious nodes? There are mainly few security techniques classified under 3 categories: cryptographic techniques, trust based techniques, and positioning techniques. Cryptographic techniques can be considered as the most reliable mechanism to guarantee integrity and availability. Hence the issue of key management has been extensively explored in the literature. The paper illustrates various key management techniques for securing MANETs [1, 2].

III. SYMMETRIC KEY MANAGEMENT SCHEMES

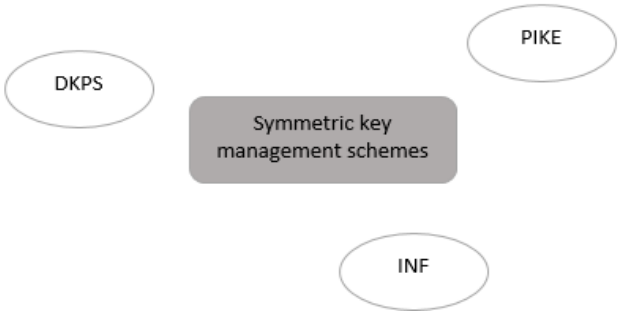

Figure 1: Symmetric Key Management Scheme

In this scheme same keys are used at both ends (sender and receiver). This key is used for encrypting data and the same key is used for decrypting data. If N is the number of communication nodes than number of keys are required are K, where K = N (N-1)/2.

DKPS (Distributed Key Pre-Distribution Scheme)

DKPS is a combination of distributed cryptographic protocols which enables the wireless nodes to perform a key distribution functions. This distribution function does not rely on any trusted third party (but the outcome is identical to trusted third party based key pre-distribution scheme). The supreme idea of DKPS is that each node's primary task is to choose a set of keys from populous publicly known key space (P). Basically DKPS contains three phases: 1. Distributed key selection (DKS): In this phase each node randomly choose keys from predefined publically known key space P to form its unique key ring ($Pi \subset P$) by using exclusion property. Which is evaluated by cover free family (CFF). 2. Secure shared key discovery (SSD): After the DKPS in this key discovery phase, each node shares the shared key to every other nodes. Node cannot find out the common keys in each one of the other nodes key rings. In this scheme the trivial method is used which is not able to provide security but it makes easier to evaluate because in DKS phase eavesdropping can be take place. 3. Key exclusion property testing (KEPT): This is the last phase of DKPS scheme. To initiate the relationship between shared keys and mobile nodes, key incidence matrix is used. In the construction of this matrix binary values will be used. This phase checks that all keys of mobile nodes comply with the exclusion property of cover free family (CFF). DKPS is more organized scheme as compared to group key agreement and also it requires less storage space as compared to pair wise key agreement method [3].

INF (Key Infection)

The basic idea of this scheme is to propagate key substantial as contact is made, somewhat like an infection growing through a biological population, each and every nodes selects the key and flood it in plaintext to its neighbors. In this scheme, nodes act as a trust component which broadcast their symmetric key. INF scheme is simpler than other symmetric key schemes yet more vulnerable to attacks. But the advantage is low storage-cost/ encryption/operation [4].

PIKE (Peer Intermediaries for Key Establishment Key Pre-Distribution Scheme)

In this scheme the nodes (trusted intermediaries) generates the shared key and it follows random key pre-distribution approach. This scheme in 2-D case (PIKE 2-D) with each of O (n) nodes every nodes distributes a secret key in two dimensions (Horizontal + Vertical). This approach can be amplified to 3D or any other dimension. The PIKE protocol also achieves the mathematical structure to intensify the connectivity of the key distribution method. The key generation is secured as long as the participating node has not been compromised. This scheme achieves good security services and trustworthy scalability [5, 6].

Discussion

By using PIKE scheme we can achieve high security and make our topology scalable. On the other hand the key infection scheme provides less security but it's capable to maintain low storage cost/operation/scalability. Conclusively, the DKPS scheme is an economical approach that need less storages than other two schemes but it contains the complex operations. So there must be a trade of remains in between. The selection of these schemes totally depends on the type of application in MANET.

IV. ASYMMETRIC KEY MANAGEMENT SCHEMES

In this scheme two keys are used at both ends (sender and receiver).that means each and every nodes have to generates two keys one will considered as a public key and other one is private key .generally Asymmetric keys are used for short-length Messages whereas symmetric keys are used for long-length messages. If N is the number of communication nodes than number of keys are required are K, where K=2N.

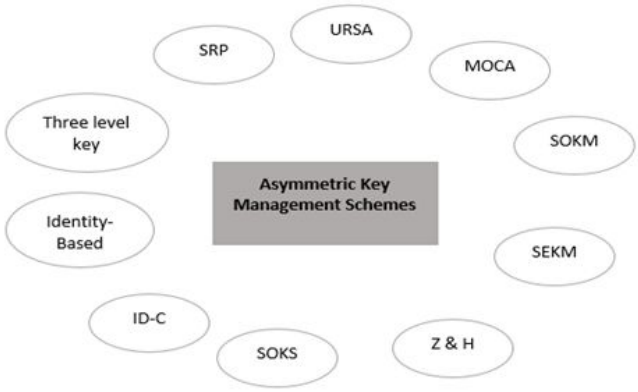

Figure 2: Asymmetric Key Management Scheme

URSA (Ubiquitous and Robust Access Control)

URSA is based on refined threshold cryptography algorithms, and the operations of these algorithms are fully

localized. This scheme provides a ubiquitous and robust access control for MANET which mainly uses ticket-based approach each trusted participant node uses a certified ticket to involve in routing and packet forwarding. If node does not have ticket than it is consider as a misbehaving/malicious node. These tickets are periodically updated. The function of centralized authority is to distribute tickets to all nodes which exist in MANET. A renewal of the tickets is done by node's neighbors rather than single ticket granting node. Node's certificate is updated by communicating with its 1-hop neighbors and it asks for partial certificate from a collection of threshold no. of mobile nodes. The outcome of this scheme is the delay in communication, search failure and also degrading the performance of the system security [7].

SEKM (Secure and Efficient Key Management)

This is the only scheme which is based on decentralized asymmetric key management approach (depends upon virtual certification Authority trust model), which provides specified, safe action for interacting and arrangement between secret resource holding authorities. This scheme is based on a set of wireless nodes which is referred as server nodes; organizing an underlying service group that each has a piece of CA's private key and can produce partial certificates. A quorum k of server can separately generate a valid certificate. The wireless nodes need the k shares of the certificate from the servers to merge them into a legitimate certificate. The ratio of server nodes is lower than the total number of wireless nodes in the network. SEKM scheme uses periodic beacons to provide a certificate services, share updates and also maintains the connection of the group. The task of managing the server group is very costly [8].

Partially Distributed Threshold CA Scheme (Z&H)

This scheme was founded by Zhou, L. and Hass, Z. in 1999. It uses the concept of trust distribution and threshold cryptography. Inside the network there are 'n' special nodes which is also called servers, each server maintains its own key pair and it is capable to store the public key of all the nodes including the servers in the network. Which allows them to communicate securely with each other all the secure services like trust management, great intrusion tolerance and offline authentication are provided by CA (certification Authority).This scheme is working same as SEKM in which each and every server node produce a partial signature by using its private key. The only difference is this scheme is able to detect a compromised server in which combiner merges all the parts of the signature [9].

Self-Organized Key Scheme (SOKS)}

The feature of this scheme is to focus on limited intrusion detection security services and it provides the offline authentication facility. Both keys (public-private keys) are produced by nodes themselves that means each node act as a CA (certification authority). In this scheme each certificate has a limited valid period issuer of a certificate that issues an update before its validity expired. If keying information resides in the certificate is correct, than at the same time node will produce the update and the operation of key authentication is performed via chains of the certificates .when user node n wants to verify the legitimacy of the public key of another user node m, they combine their local certificate repositories and n evaluates the legitimacy of Km (public key which belongs to given user m; Km is bound to m by the signature of n) based on the certificates.

It accommodates in the merged repository. The major drawback of this scheme is the poor resource efficiency and the poor scalability but it has high integrant encryption operations and high storage cost [10].

Key Distribution Technique (ID-C)

In this scheme during the network formation each and every nodes produce a master public key in distributed manner. It is available to every node into the network a public key used for encryption which is produced by a master public key and individual node's ID. Similarly by combining the master private key and the nodes ID a node's private key is obtained.so in these approach nodes is using its IDs to generate keys. The module of private key generator performs an important role in this scheme [11, 12].

Identity-Based Asymmetric Key Management Scheme

Generally this scheme consist four layers of key exchange process. Initialization, registration, verification and key exchange

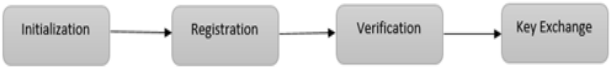

Figure 3: Identity-Based Key Asymmetric Management Scheme

In this scheme Public-private key pair is produced by RSA method and each node acquires its long term private-public key pair. A key generation center randomly chooses the secret key as a master key and also publishes its suitable public key. In the registration layer, each user sends its ID to the key generation center that provides him with his signature. Where in the verification phase, user who wants to communicate will challenge each other before producing the session keys in the next key exchange layer [13] - [15]

SRP (Secure Routing Protocol)

The scheme is composed with three nodes (client nodes, server nodes, combiner nodes) and an administrative authority works as a trader which provides initial certificate to the mobile nodes. Client nodes are normal user's nodes in MANET, while the server nodes are responsible to produce a partial certificates and storing it to the directory. Here, the server node is performing a part of CA and the last combiner node performs important task in the scheme, it combines those partial certificates which produced by server node into the valid certificate [5].

Three Level Key Management Scheme

This scheme is based on threshold three level key management and identity- based scheme which adopts elliptic curve cryptography (ECC) and Bilinear pairing computation. In this scheme, when new node enters in MANET, its first task is to perform authentication operation with its neighboring nodes before all the nodes in the cluster can start a private key generation service(PKG), in which a new master public key is used in identity-based cryptosystem and a master private key is shared among the nodes. They all are in threshold (t-out-of-n) fashion. Means at least t number of nodes required to recover the new master secret key. Then the new node can acquire its corresponding personal private key by sharing their private keys from each of the t number of nodes which are forming PKG. new node acquires its personal public key by applying one way hash function and its own identity. Here, in this scheme bilinear maps are applied to cryptography in order to achieve more efficiency and security [16, 17].

Mobile Certificate Authority (MOCA)

In this scheme the healthy nodes is used as MOCA nodes, here healthy in terms of the node contains more

computational power and it is physically more secure than the other nodes in the MANET. When nodes are equally healthy than the MOCA nodes are randomly chosen from the MANET. This approach is decentralized and all the task of CA is distributed to MOCA nodes [18].

Self-organized Key Management (SOKM)

In this scheme there are two repositories exist, updated certificate repository and non-updated certificate repository. Each node maintains non-updated repositories for calculating certificate graph. In this scheme each and every node generates public key certificate to other wireless nodes and every node act as their own repository for key authentication process. Public key chain certificate method is used in this model [19].

Discussion

In this section we illustrated the different key management schemes which use asymmetric approach in MANET. The selection of the suitable scheme is totally based on the application for example, the URSA scheme is capable to encrypt local communication and it provides availability and reliability. This kind of scheme is used in like military level applications, traffic surveillance systems etc. On the other hand ID-C scheme uses intrusion tolerances, trust management and off net authentication type security services, ID-C enables network to achieve scalability by this scheme. Scalability is achieved through Id-Revocation list with great resource efficiency. Also this scheme has less operations, medium encryption, storage space and intermediates. So this kind of scheme would be the best for commercial or agricultural applications.

V. GROUP KEY MANAGEMENT SCHEMES

Group key is a distinctive parameter that is assigned to group of mobile nodes in MANET. In order to distribute a group key to particular group, first of all the group needs to be created and then after key distribution operation take place to all the members which resides in this group.

Simple and Efficient Group Key Management(SEGK)

Yuhong Dong, Jie Wu, Bing Wu has found SEGK approach in 2008. In this scheme, to achieve efficiency and fault tolerance two multicast trees are formed parallel. All the work is substituted on one tree if other tree is broken. In this scheme, one tree is considered as a blue tree and the other one as a red tree. The connection of tree is handled by coordinator. It does distribution and computation of intermediates keying materials to all members via underlying tree links. To generate the common group key each mobile node in group participates in a collaboration of an ultimate common group key which is refreshed periodically.

The initialization process starts by the group initiator (also known as the group coordinator) by flooding an advertisement message in the network. The computation cost is directly proportional to the number of mobile nodes. The node can choose fix color according to the following situations:

If **Total number of neighbor nodes < Primarily defined threshold value,** will choose the Grey color

If probability = 0.5, than node choose blue or Red color

In SEGK scheme, any group member or mobile node can leave and join the network. It assumed that all the nodes contain the valid certificate before entering into the network. PKI is required to manage these certificates. Two detection

techniques are elaborate in this scheme; (a) Tree Links (b) Periodic broadcasting of control Messages [20, 21].

VI. HYBRID OR COMPOSITE KEY MANAGEMENT

Hybrid or composite keys are a union of symmetric and asymmetric keys. Instead of one, this scheme is works on two keys which can cause an issue for MANETs

Cluster Based Composite Key Management

In this scheme the entire network is partitioned into clusters. For each cluster the node with having maximum trust ability is selected as a cluster head (CH) by Network Administrator. In every cluster K nodes are selected as public key generation (PKG) nodes which are having high trust values. Nodes are able to Join and leave the cluster. Thse task of CA is assigning the ID to each node, prior it joining to the network which also contains the self-assigned public key. Storing the node information and certificate revocation is handled by Mobile agent (MA).When the new node registers its information in the cluster head at that time PKG nodes produce its private key shares and later those shares are managed by the cluster head. Public key of cluster head is computed from the current trust value and the old Public key and it is known to all the members of the cluster.

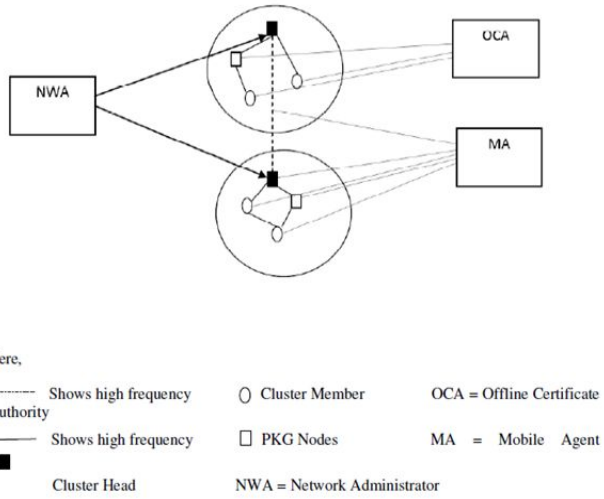

Figure 4: Cluster based Composite Key Management [25]

To communicate between cluster member the system uses a low frequency and to communicate between two cluster head the system uses high frequency [22].

Zone-Based Key Management Scheme

This model is totally based on Zone routing protocol (ZRP) in which entire network is divided into zones. For inter-zone communication asymmetric key and for intra-zone communication symmetric key is used between nodes. In this scheme a threshold cryptography is used for certificate production and for symmetric key production the Diffie-Hellman scheme is used [23, 24].

Discussion

The described schemes can be further categorized into fully self-organized MANETs and authority-based MANETs. The previous scheme do not contain any online or offline authority while in the later scheme the trusted

authority handles the nodes before the network formation due to the chaotic nature of MANETs there must be a trade-off remains between the security and complexity, so the selection of the proper scheme is totally based upon type of the application. It is true that group key is less bulky and efficient because it uses only one key pairs but on the other hand it is more vulnerable and lack of confidentiality between the different nodes. In the end the hybrid key management schemes are more secure as compared to symmetric and asymmetric key management schemes but on the other hand the scheme requires more operations regarding the maintenance and production of the keys because this scheme contains two keys instead of one.

VII. CONCLUSIONS & FUTURE WORK

In this paper, different type of key management schemes in MANET has been covered. We categorized the schemes into four parts depending on the type of key used. We illustrated three types of symmetric key management schemes: DKPS, PIKE and INF. In which DKPS is more efficient and secure key management scheme. In asymmetric approach, ID-based key management scheme is more reliable due to its scalable nature. Further, the SEGK group key management scheme contains double multicast tree which improves efficiency and it maintains in a parallel fashion. The cluster based and zone based are dependent on Hybrid key management schemes, which are more complex but more secure than other schemes. In future work, we will focus on particular key management scheme and try to modify it and add that scheme to specific MANET protocol and also we would implement it in real world application.

REFERENCES

1. Sharma, Shilpi Burman, and Nidhi Chauhan. "Security issues and their solutions in MANET." Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), 2015 International Conference on. IEEE, 2015.
2. Sheikh, Rashid, Mahakal Singh Chande, and Durgesh Kumar Mishra. "Security issues in MANET: A review." Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference On. IEEE, 2010.
3. Chan, Aldar C-F. "Distributed symmetric key management for mobile ad hoc networks." INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies. Vol. 4. IEEE, 2004.
4. Anderson, Ross, Haowen Chan, and Adrian Perrig. "Key infection: Smart trust for smart dust." Network Protocols, 2004. ICNP 2004. Proceedings of the 12th IEEE International Conference on. IEEE, 2004.
5. Chan, Haowen, and Adrian Perrig. "PIKE: Peer intermediaries for key establishment in sensor networks." INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE. Vol. 1. IEEE, 2005.
6. Aziz, Baayer, Enneya Nourdine, and E-K. Mohamed. "A recent survey on key management schemes in manet." Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on. IEEE, 2008.
7. Luo, Haiyun, et al. "URSA: ubiquitous and robust access control for mobile ad hoc networks." IEEE/ACM Transactions on Networking (ToN) 12.6 (2004): 1049-1063.

8. Wu, Bing, et al. "Secure and efficient key management in mobile ad hoc networks." Journal of Network and Computer Applications 30.3 (2007): 937-954.
9. Zhou, Lidong, and Zygmunt J. Haas. "Securing ad hoc networks." Network, IEEE 13.6 (1999): 24-30.
10. Capkun, Srdjan, Levente Buttya, and Jean-Pierre Hubaux. "Self-organized public-key management for mobile ad hoc networks." Mobile Computing, IEEE Transactions on 2.1 (2003): 52-64.
11. Han, Kyusuk, et al. "A scalable and efficient key escrow model for lawful interception of IDBC-based secure communication." International Journal of Communication Systems 24.4 (2011): 461-472.
12. Khalili, Aram, Jonathan Katz, and William Arbaugh. "Toward secure key distribution in truly ad-hoc networks." Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on. IEEE, 2003.
13. Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 1996.
14. Han, Kyusuk, et al. "A scalable and efficient key escrow model for lawful interception of IDBC-based secure communication." International Journal of Communication Systems 24.4 (2011): 461-472.
15. Kapil, Anil, and Sanjeev Rana. "Identity-Based Key Management in MANETs using Public Key Cryptography." International Journal of Security (IJS) 3.1 (2009): 1-26.
16. Xiong, Wan An, and Yao Huan Gong. "Secure and highly efficient three level key management scheme for MANET." WSEAS Trans. Comput 10.1 (2011): 6-15.
17. Okamoto, Tatsuaki. "Cryptography based on bilinear maps." Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Springer Berlin Heidelberg, 2006. 35-50.
18. Yi, Seung, Prasad Naldurg, and Robin Kravets. "Security-aware ad hoc routing for wireless networks." Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking \& computing. ACM, 2001.
19. del Valle, Gerardo, and Roberto Gómez Cárdenas. "Overview the key management in ad hoc networks." Advanced Distributed Systems. Springer Berlin Heidelberg, 2005. 397-406.
20. Yeun, Chan Yeob, et al. "Secure authenticated group key agreement protocol in the MANET environment." information security technical report 13.3 (2008): 158-164.
21. Wu, Bing, Jie Wu, and Yuhong Dong. "An efficient group key management scheme for mobile ad hoc networks." International Journal of Security and Networks 4.1-2 (2009): 125-134.
22. PushpaLakshmi, R., and A. Vincent Antony Kumar. "Cluster Based Composite Key Management in Mobile Ad Hoc Networks." update 4 (2010): 10.
23. Haas, Zygmunt J., Marc R. Pearlman, and Prince Samar. "The zone routing protocol (ZRP) for ad hoc networks." draft-ietf-manet-zone-zrp-04. txt (2002).
24. Arabia, Sudia. "A HYBRID SCHEMA ZONE-BASED KEY MANAGEMENT FOR MANETS." Journal of Theoretical and Applied Information Technology35.2 (2012).

25. Dalal, Renu, Yudhvir Singh, and Manju Khari. "A review on key management schemes in MANET." International Journal of Distributed and Parallel Systems3.4 (2012): 165.

26. Perkins, Charles E. Ad hoc networking. Addison-Wesley Professional, 2008.