A Review on Key Management Schemes in MANET

Renu Dalal[1#],Yudhvir Singh[2] and Manju Khari[1]

[1]Computer Science & Engg. Department, Ambedkar Institute of Technology,
New Delhi, India.
[2] Department of Computer Science & Engg, U.I.E.T M.D University Rohtak, India
[#]Corresponding Author: dalalrenu1987@gmail.com

Abstract

Mobile Ad-hoc network is spontaneous and infrastructure less network, which consist of wireless mobile nodes. MANET is formed on-the-fly and also provides various operations like packet forwarding, routing, network management, communication, etc between mobile nodes. MANET is one of the types of wireless network, in which any mobile node can join the network and leave the network in dynamic period. Mobile ad-hoc network doesn't having centralized infrastructure and due to its basic characteristics this network is very vulnerable to attack. There are lots of trust models and routing protocol which are used in MANETs to achieve security. Different trust schemes are used to provide confidentiality, integrity and availability in mobile ad-hoc network to gain the secure environment. In this paper, we present the study on various kinds of key management schemes with their special features.

Keywords

Key, INF, SOKM, SEGK, Three Level Key and DKPS

1. Introduction

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. In MANET speed variesdepending upon the applications, for example, in commercial application (short range network) speed is high but in military application (long range network) speed is low, i.e. speed is inversely prepositional to network range. MANET have special features like network can work in standalone intranet as well as can be connected to large internet, it can cover the areabigger than a transmission range and by using internal routing can be rapidly deployable etc. Different cryptographic keys 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 forencryption 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

DOI : 10.5121/ijdps.2012.3417

encryptionand 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. Asymmetric keys are used for short messages but symmetric keys are used for long messages If n nodes wants to communicate in MANET, k number of keys are needed, where k =2n.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 [1]. There are specifically three categories of group key protocol 1. Centralized, inwhich 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.

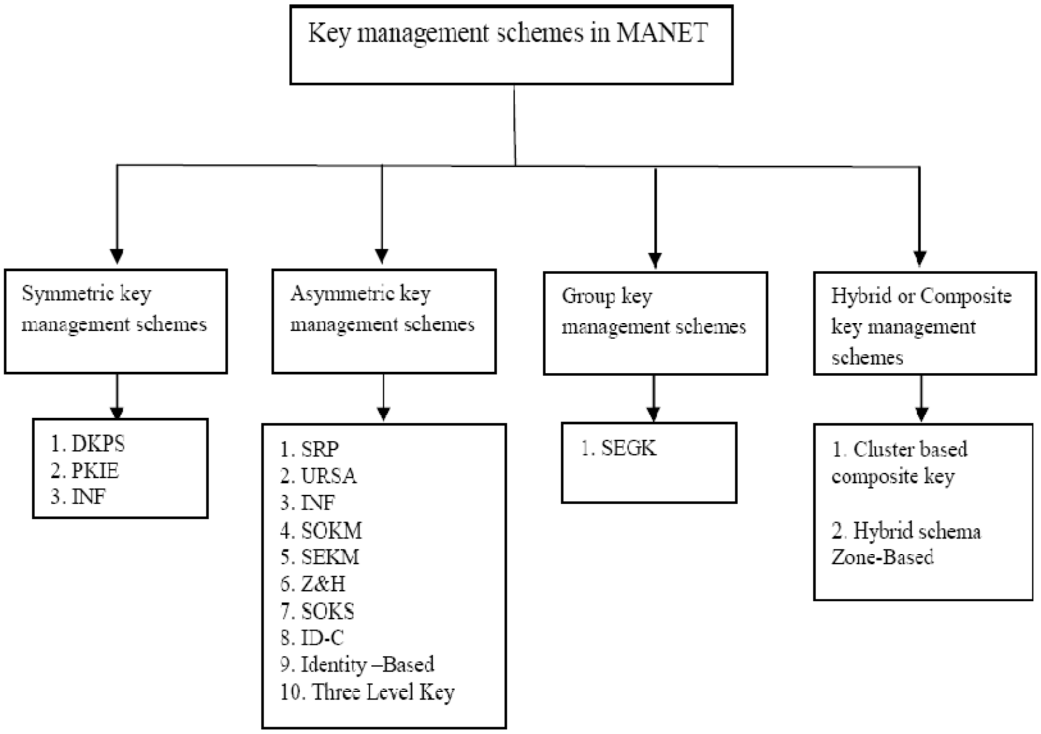
Key management schemes in MANET
Symmetric key management schemes
Asymmetric key management schemes
Group key management schemes
Hybrid or Composite key management schemes
1. DKPS
2. PKIE
3. INF
1. SRP
2. URSA
3. INF
4. SOKM
5. SEKM
6. Z&H
7. SOKS
8. ID-C
9. Identity –Based
10. Three Level Key
1. SEGK
1. Cluster based composite key
2. Hybrid schema Zone-Based

Figure 1 Key Schemes in MANET

Initialization of system users with in a network, generation, distribution, installation, control, revocation, destruction, storage, backup, archival, bootstrapping and maintenance of trust in keys are different services which are important for security of the networking system. 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. The study about the different types of key management schemes are given in this paper. Figure (1) shows the different existing key management schemes for MANET.

2. Symmetric Key Management Schemes in MANET

(A) 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.Cover Free Family (CFF) concept is using for evaluating the exclusion property, to make a CFF in distributed manner probabilistic method is used. This technique removes the need of TTP (trusted third party) and makes the MANET more dynamic. 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. KEPT phase test that is all keys of mobile nodes fulfilling the exclusion property of CFF. Features of DKPS are no need of TTP. DKPS needs less storage as compared to pair-wise key agreement approach. This scheme is more efficient as compared to group key agreement [2].

(B) 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 [3].

(C) 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 [4].

3. Asymmetric Key Management Schemes in MANET

(A) Secure Routing Protocol (SRP):-This scheme is composed with three nodes and an administrative authority which work as dealer in this model. Dealer is the entity which provides the initial certificate to the mobile nodes. Three nodes are defined as: 1. Client Node: Client nodes are the normal user’s mobile nodes that wanted to came in MANET. 2. Server Node: The responsibility of generating the partial certificates and storing the certificates in directory structure through which mobile nodes can request for the certificates of other mobile nodes. Here Server Node is the part of certificate authority (CA). 3. Combiner Node:- This node plays the important task in SRP model, Combiner Node combines the partial certificate into the valid certificate.

(B) Ubiquitous and Robust Access Control (URSA):URSA is efficient and provides reliable availability with having the feature of encrypted local communication. This model uses efficient threshold scheme to broadcast the certificate (RSA Certificate)signing keys to all mobile nodes. Each mobile node of MANET updates their certificates periodically. The functionality of CA is distributed to all mobile nodes which existing in MANET. If any mobile node wants to update their certificate than, that node should be contact to 1-hop neighbors and request partial certificates from a collection of threshold k no. of mobile nodes. This scheme generates communication delay, search failure, and degrades the system security. To protect the network from DOS attack and the compromise the signing key URSA using verifiable and proactive secret sharing mechanisms [6].

(C)Mobile Certificate Authority (MOCA):- The mobile nodes which having great computational power, physically more secure and on the basis of heterogeneity those mobile nodes used as MOCA nodes in this asymmetric key management scheme. When the nodes are equally equipped than, MOCA nodes are selected randomly from the MANET. This scheme is decentralized and the services of CA are distributed to MOCA nodes (subset of mobile nodes). To find out the safe path in the network is the crucial task in MOCA asymmetric key management scheme [7].

(D) Self-Organized Key Management (SOKM):SOKM model using two local certificate repositories one is updated and another one is non updatedcertificate 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[5].

(E)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. Thismodel 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 groupand for share updates SEKM using periodic beacons. The cost of maintaining the structure server group is high [8].

(F)Partially Distributed Threshold CA Scheme (Z&H): Partially Distributed Threshold CA Scheme was discovered by Zhou, L. and Hass, Z. in 1999. When the mobile ad-hoc network is constructed, this scheme is using the concept of CA distribution in threshold fashion. Security services like off line authentication, great intrusion tolerance, and trust management by CA (certification authority) are provided by Z&H asymmetric key management scheme. The key is generated by this model are accepted by self organized network (MANET) and partial distributed threshold CA. The survivability of resources efficiency is poor but it having the scalability of CRL (certificate revocation list), and certification [9].

(G) Self Organized Key Scheme (SOKS): In the self organized network each mobile node acts as a distinct CA.SOKS was disclosed by Capkun, S., Buttya, L., and Hubaux, P. in 2003. It has poor scalability and poor resource efficiency but having the off line authentication and limited intrusion detection security services. SOKS having high intermediates encryption operations and high storage cost [10].

(H) Key Distribution Technique (ID-C):- Set of mobile nodes creates or initialize the MANET with using the threshold private key generator identity based scheme. The generated key is accepted by self organized network. Off net authentication, trust management and intrusion tolerances type security services are provided by ID-C asymmetric key management scheme. Scalability is provided through Id Revocation list with great resources efficiency. This scheme having medium intermediates, operation, encryption and storage cost [11].

(I) Identity-Based Key Asymmetric Management Scheme:Without using the environment of PKI Secure Identity-Based Key management scheme is proposed by Anil Kapil&SnjeevRana. This scheme consisted with four phases. To verify the user identity and generating the corresponding private keys this scheme needs trusted key generation centre. Figure (2) presents the view of Identity-Based Key Management model Where; I = Initialization Phase, R = Registration Phase, V = Verification Phase, and K = Key Exchange Phase.

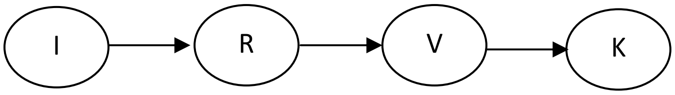

Figure 2 Identity-Based Key Asymmetric Management Scheme

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 [12].

(J) Three Level Key Management Scheme: Secure and Highly Efficient Three Level Key Management scheme for MANET is proposed by Wan AnXiong, Yao Huan Gong in 2011. To achieve three level security in MANET, this model uses ID-Based Cryptography with threshold secret sharing, Elliptive Curve Cryptography (ECC) and Bilinear Pairing Computation. ECC provides small keys to mobile nodes and high security level. Key generation and key distribution security services with the prevention from adversaries attack are done by (t, n) threshold secret sharing algorithm. ECC provides enhanced security level with using 160 bits key and 1024 bits equivalent strength of RSA. Pairing technology provides confidentiality and authentication with less computational cost and reduced communication overhead [13].

4. Group Key Management Schemes in MANET

(A) Simple and Efficient Group Key Management (SEGK): Bing Wu, Jie Wu, and Yuhong Dong were disclosed the SEGK model in 2008. 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 andanother 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. The node can choose the red, blue and grey color accordingto the following situations:-

If Total no of neighbors < Predefined Threshold Value, than node will chose the **Grey Color.**

If probability = 0.5, than node will chose the **Red or Blue Color.**

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 [1].

5. Hybrid or Composite Key Management Schemes in MANET

(A) Cluster Based Composite Key Management:-This model is disclosed by R.PushpaLakshmi and A. Vincent Antony Kumar in 2010. 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. Overview of cluster based composite key management scheme presented in figure (3).

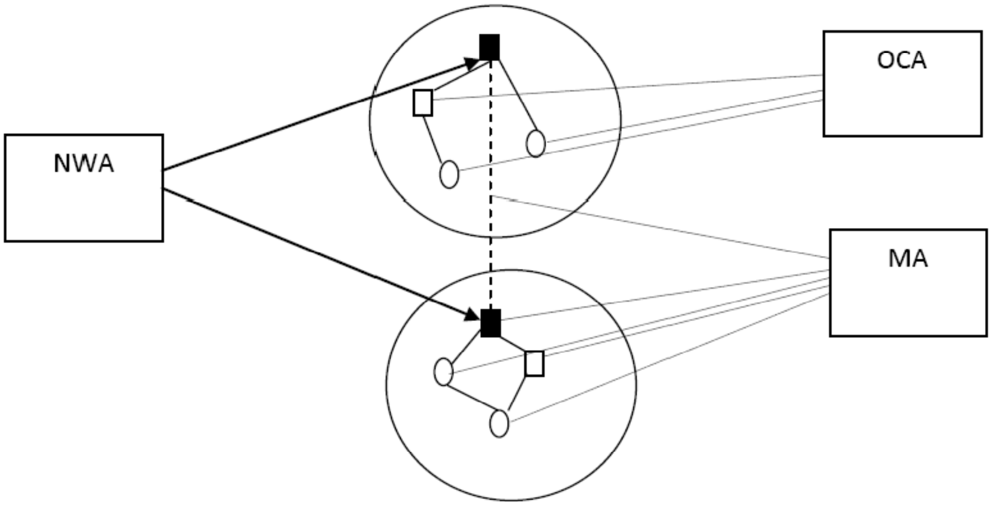

Figure 3 Cluster Based Composite Key Management

Here,

┈┈┈┈ Shows high frequency ○ Cluster Member OCA = Offline Certificate Authority

——— Shows high frequency □ PKG Nodes MA = Mobile Agent

■ Cluster Head NWA = Network Administrator

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 [14].

(B) Zone-Based Key Management Scheme:- This scheme using ZRP (Zone Routing Protocol) and the work of [15,16]. This model is proposed by ThairKhdour and Abdullah Aref in 2012, 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 rzone (zone redius). Without depends on clustering mobile node uses asymmetric key management for inter-zone security. It provides efficient way to making thepublic key without losing the capability of making the certificates [17].

6. Conclusion & Future Work

Different types of key management schemes are covered in this survey paper. In summary, symmetric key management schemes are described in three categories DKPS, PIKE and INF. DKPS symmetric key management scheme is much efficient as compared to group key schemes and pair wise key agreement. PIKE scheme have good security services with fair scalability. INF model have no need of collaboration effort with having low storage cost. This paper concludes that DKPS is highly secure and efficient schemes as compared to other symmetric key management schemes. Every type of asymmetric key scheme is described in a section 2. The identity-based key management is reliable and takes four phases, I, R, V and K which described in section 3. SEGK is group key scheme in MANET; double multicast tree is constructed in this model. This blue and red multicast tree improves efficiency and it maintains in a parallel fashion. Two detection methods are introduced in SEGK scheme. Cluster based & Zone based key schemes come in hybrid or composite key management scheme. In future work, we will focus in a particular key management scheme deeply and try to make a new key management scheme.

References

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

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

3] Aziz, B., Nourdine, E. and Mohamed, E., "A Recent Survey on Key management Schemes in MANET"ICTTA'08, pp. 1-6, 2008.

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

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

[6] Luo, H. and Lu, S., "URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks", IEEE / ACM Transactions on Networking Vol. 12, pp. 1049-1063, 2004.

[7] Yi, S., Naldurg, P. and Kravets , R, “Security-aware ad hoc routing for wireless networks ”, MobiHoc, pp. 299-302, 2001.

[8] 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.

[9] Zhou, L. and Hass, Z.,”Secure Ad Hoc Networks”, IEEE Network Magazine vol. 13, no. 6, pp. 24-30, 1999.

[10] Capkun, S., Buttya, L., and Hubaux, P.,”Self-Organized Public Key Management for Mobile Ad Hoc Networks”, IEEE Trans. Mobile Computing, vol. 2, no. 1, pp. 52-64, 2003.

[11] A. Khalili, Katz, Jonathan and Arbaugh, William A.,” Towards secure key distribution in truly ad hoc networks”, IEEE Workshop on Security and Assurance in ad hoc Networks – in conjunction with the 2003 International Symposium on Application and the Internet, 2003.

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

[13] Wan AnXoing, Yao Huan Gong, “Secure and Highly Efficient Three Level Key Management Scheme for MANET”, WSEAS TRANSACTIONS on COMPUTERS, Vol. 10, Issue 10, 2011.

[14] 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.

[15] Balasubramanian A., Misha, S., Sridhar, R., “A Hybrid approach to key management for enhanced security in ad hoc networks”, Technical report, university at Buffalo, NY, USA,2004.

[16] Balasubramanian A., Misha, S., Sridhar, R., “Analysis of a hybrid key management solution for ad hoc networks IEEE WCNC’05, vol. 4, PP. 2082- 2087, 2005.

[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.