A REVIEW ON EFFICIENT KEY MANAGEMENT SCHEMES FOR SECURE ROUTING IN MOBILE AD HOC NETWORKS

C.Krishna Priya1, Prof.B.Satyanarayana 2

1 Research Scholar, Department of Computer Science & Technology, Sri Krishnadevaraya University, Anantapur
2 Professor, Department of Computer Science & Technology, Sri Krishnadevaraya University, Anantapur
krishnapriyarams@gmail.com, bachalasatya@yahoo.com

ABSTRACT:

Mobile Ad Hoc Networks (MANETs) have become ubiquitous in revolution of computing as they are suitable for on demand communication scenarios. However, they are vulnerable to attacks due to their multi-hop, dynamic, mobility and resource constrained nature. It is the most sensitive issue faced by MANETs. Especially, it is so in the absence of key management system. Therefore reliable key management scheme is indispensable to secure communication between the nodes in MANET besides ensuring authentication, non repudiation, confidentiality and integrity. Key management schemes play a pivotal role in distributing keys among routing protocol, and participating nodes in communication. As the network lacks infrastructure and central server, efficient key management is a challenging and open problem to be addressed. Moreover nodes in MANET are dynamically configured without a fixed topology which causes less than ideal trust relationship among nodes. As a matter of fact every node in the network plays a role of an intermediate router. This makes the nodes to be more responsible, reliable and able to participate in key management schemes for robust, highly efficient and secure communication. The knowledge of the present state-of-the-art on efficient key management in MANETs can help in securing networks and move on to further enhancements in the area. Towards this end, in this paper, we analyze various key management schemes and evaluate them in terms of their utility, and performance in the real world networks.

KEYWORDS - Mobile Ad Hoc Networks, secure routing, key management schemes

[1] INTRODUCTION

MANET is an infrastructure less network which is established automatically on demand. It is a set of wireless nodes that are configured automatically on the fly thus making it suitable candidate as it is useful in emergency situations [1], [2]. In other words it is a multi-hop communication network organized temporarily with nodes that have receivers and transmitters [3]. The topology of network is dynamic which is created and modified on the fly [4]. MANET supports many routing protocols such as Dynamic MANET On-demand routing protocol (DYMO), Optimized Link State Routing protocol (OLSR), Destination Sequenced Distance Vector (DSDV), Dynamic Source Routing (DSR) and Ad Hoc On-demand Vector Routing (AODV). Mobility is the fundamental difference between other networks and MANET [5]. Wireless Sensor Network (WSN) traffic also can be relayed over MANET. It does mean that WSN communications are possible between devices of MANET [6]. MANET supports TCP/IP protocol to integrate communication with wired networks as well [1]. Every node in MANET acts as a host in the network and also
router which can cooperate in communication [7]. As MANET topology is dynamic in nature which makes the procedure of routing more difficult and vulnerable to Denial of Service (DoS) attacks such as flooding which results in network congestion [8]. MANETs are vulnerable to attacks such as location disclosure, black hole, replay, work hole, blackmail, denial of service and routing table poisoning.

Secure key management is essential in MANETs to protect sensitive communications in the network besides withstanding various kinds of attacks specified earlier. The key management protocols are classified into many types as shown in figure 1.

Pairwise key approach is the approach in which key server provides pairwise keys to every participant. One such model is GKMP. Apart from pairwise key the participants also know group key and group key encryption key. Secure Locks is a key management protocol where a key server uses only one broadcast to make a new group key or change existing one for all members in the group. Hierarchy of keys approach is most efficient but has tradeoff with storage. Here, in addition to pairwise keys, the key server also shares keys with subgroups. Ring based cooperation is found in CLIQUES protocol. It treats group members as controllers. One of the controllers collects contributions from group members and then adds its own contribution. Afterwards it broadcasts it to all group members to enable them generate group key. In hierarchical based cooperation a structure is followed to group members. For instance STR protocol uses a tree structure that is used in the cooperative communications. Broadcast based cooperation has fixed number of rounds. In BD protocol [10] intermediate values are broadcasted to all participants and the load is shared across parties. Based on the way clusters are formed the decentralized approaches are named static clustering and dynamic clustering. A consequence based classification of attacks in MANET includes denial of service, sleep deprivation, selfishness, network partition, routing loops, and black hole [11]. Reputation Trust (RT) model is proposed by Rizivi et al. in order to increase credibility of nodes and reduce malicious behavior in MANET [12].
Routing Protocols in MANET

Routing protocols play an important role in securing MANETs. A summary of such protocols is appropriate to mention here. Figure 1 shows the protocols available for MANETs.

Security Requirements in MANETs

According to Yang et al. [13] security issues are to be addressed in such a way that it protects the whole protocol stack. In the application layer the security issues include abuses, malicious codes, worms and viruses. In transport layer authentication, end-to-end communication through cryptography is the issues. In Network layer the issues include the protection of routing and forwarding protocols. Link layer security issue is protecting MAC protocol. Prevention of attacks such as Denial of Service (DoS) and jamming attacks are issues in physical layer. They further classified multifence security solutions for MANETs. The components of these solutions are as show in figure 3.

Fig. 2 –Routing protocols in MANETs [12]

Fig. 3 – Components of multifense security solution [13]
A Review on Efficient Key Management Schemes for Secure Routing in Mobile Ad hoc Networks

As summarized in figure 3, the components in multifense security solution belong to either link-layer security solutions or network layer security solutions. Secure ad hoc routing, proactive protection through message authentication primitives, secure packet forwarding, reactive protection through detection and reaction, source routing, link-state routing, distance vector routing, misbehavior detection, misbehavior reaction are the solutions that can be made in network layer. Whereas the link layer security solutions include using next generation WEP, altering cryptographic primitives to fix loop holes. In this paper we provide the present state of the art with respect to key management schemes. Our contribution in this paper is the survey of various key management schemes existed for security MANET communications. The remainder of the paper is structured as follows. In section II, we review literature on key management schemes in MANETs. In section III we evaluate the schemes that have been reviewed while section IV concludes the paper.

[2] KEY MANAGEMENT SCHEMES FOR MANETs

This section reviews available key management schemes for secure routing in mobile ad hoc networks. It focuses on the cluster based key management schemes, threshold secret sharing, besides many other key management schemes that are suitable for various MANET applications in varied mobility scenarios.

Cluster Based Key Management for MANET

Hai-tao [14] proposed cluster based key management scheme. It is built in a distributed network as soon as the network is initialized. The network is divided into clusters with cluster head (CH) in each cluster. At the time of initialization CH generates share key for the cluster. The shadow of cluster key is securely distributed to every other node in the cluster through nonce. CH is also capable of determining whether a node originally joins cluster or comes from other cluster (roaming node). If that is a roaming node, CH gets its history through its old CH node and then makes a decision to allow the node or deny it. This key management scheme is proved to be efficient, secure, fault tolerant and expansive in nature.

Threshold Secret Sharing

Cho et al. [15] proposed a secure mechanism for key management. They achieved it through regeneration of Cryptographically Generated Addresses (CGA). The CGA regeneration is done using threshold secret sharing. They considered MANET with IP v6 addressing scheme. Certificate Authorities are not used in MANETs. Instead of CA Threshold Secret Sharing (TSS) is used. The TSS facilitates dividing of cryptographic primitives into n number of pieces and associate them with n participants. Out of the n pieces if t number of pieces are gathered it is possible to establish secret data. However, if t-1 pieces are gathered it is impossible to reconstruct secret data. As the secret data is distributed it gives more security. For secure neighbor discovery here is based on CGA and digital signature. The CGA format is as shown in figure 4.
When a private key is compromised, the CGA regenerates address. The regeneration process is done based on TSS which provides certificate issuing service. The TSS mechanism can help nodes to identify compromised nodes in the network. As per this security mechanism each node in MANET can have a secret share, public key pair and a certificate. Without the presence of CAs, this mechanism obtains certificates using the TSS mechanism. Authentication of a sender and the message is done by the security mechanism. Public key cryptography, IP v6 and CGA work together to make the security more robust to attacks. The security mechanism has provision for preventing brute-force attacks. This approach is capable of providing fool proof security. CGA can also prevent IP address spoofing attack.

**Threshold ID-Based Public-Key Management**

A threshold ID based public key management scheme was proposed by Deng et al. [16]. The nodes initially existed in MANET generate security keys in collaborative fashion. The keys are not kept in any single node. An assumption made in this scheme is that each node in the network has a unique ID. The whole system private key is made up of all partial keys of all nodes in the network. Each node obtains partial system private key with respect to its own identity. A part of system private key is shared to each node based on the ID of the node in the network. A threshold is used nodes while generating private keys of other nodes. To the given identity a set of nodes together can generate security key. The generated secret keys are securely transmitted. While sending a request message, the requesting node is supposed to present self generated public key which is temporary. Such public key is used by the issuing nodes.

**Public Key Management Scheme for MANETs**

Yuh-Min Tseng [17] proposed a scheme for key management in MANETs. This scheme has two phases namely initial phase and certificate distribution phase. In the first phase the MANET is established using cluster-based networking where the nodes form clusters with cluster heads. In the second phase actually takes care of certificate distribution that will ensure secure
communications in MANET. The schematic diagram showing ad hoc network which is cluster-based is as given in figure 5.

![Ad Hoc Network](image)

**Fig. 5 –MANET integrated with heterogeneous network [17]**

As seen in figure 5, in the initial phase, the clusters are formed which are connected to a network which is integrated with a heterogeneous network. Each cluster has a cluster head for proper communication. The network has nodes and agent nodes. Connecting information is shared by all nodes. The CH also announces its CI to neighboring nodes. In the certificate distribution phase uses two protocols. The first protocol has two components such as CH and authentication server as visible in figure 5. First of all CH assesses the connectivity to server. Then CH randomly chooses secret key and compute public key. On receiving a request, the CH processes the request after due verification through security certificates. The second protocol is similar to that of the first protocol but it is purely used for certificate distribution for general nodes. Their results revealed that the scheme is capable of preventing passive attack, guessing attack, and identity confirmation of concrete nodes.

**Other Key Management Schemes**

Capkun et al. [18] proposed a key management scheme that needs human intervention in order to create security channels. Then it supports exchange of public keys between the nodes that participate in communication. The scheme has high mobility support. In all scenarios where there are frequent communications between parties this scheme can be used. Proposed a scheme which is similar to that of [18] but it supports low mobility and suitable when participants are in the same physical space. The key management scheme proposed is also similar to that of [18] but its usage is limited to master-slave relationships. Proposed a scheme that is suitable for high mobility environments. In this scheme TESLA keys are distributed to all the nodes that participate in communication. For this it has special online key distribution center for secure key distribution. It ensures ahead of time synchronization of keys between sender and receiver. This scheme is very useful when there is need for source authentication of broadcast messages. The scheme proposed uses a common password between parties which needs human intervention. It facilitates key exchanges between two parties or even among a group of participants as well. However, it works well when nodes in MANET exhibit low mobility. It is best suited for communications in room meetings. Presented a key management scheme that is suitable in the environments where non-hierarchical applications are used. It is also suitable when high mobility
is with MANET nodes. Here secure key distribution is made possible through transitive trust among all participating nodes in the communication. Non-hierarchical applications of MANET can also use the key management scheme proposed which works in high mobility environment. The security is initiated trusted authority by distributing private key shares to $t + 1$ node. Private Key shares are associated with identity keys that cannot be changed by nodes participating in secure communications. Proposed a scheme specially meant for MANETs which are used in military applications or such emergency applications. This scheme supports medium mobility support. The scheme is very secure. A Trusted Authority (TA) is part of the scheme. The nodes in MANET are provided private key shares which are from CA. The TA coordinates the security mechanism. Within two consecutive share refreshing processes, $t+1$ CA nodes cannot be compromised by a mobile attacker. Thus it provides fool proof security.

Vennila and Duraisamy [19] proposed a multi-level group key management scheme. Their scheme is used for secure multicasting in MANETs. The technique works in hierarchical fashion by giving priority to cluster heads over cluster members. Cluster heads (CHs) are formed based on the highest bandwidth availability and residual energy. The cluster head which has been elected acts as group leader (GL) for multicasting. One way function chain is used to generate keys. Using shuffle algorithm, key distribution is done. Assuming the presence of attackers, experiments are made in terms of delivery ratio, drop of packets, energy, and resilience. This scheme is energy efficient and improves packet delivery ratio.

Lakshmi, Sajid and Ramana [20] studied energy efficiency and security in MANETs. They have provided details of various protocols such as Ad Hoc On-demand Vector Routing (AODV), Temporally Ordered Routing (TORA), Dynamic Source Routing (DSR), and Destination-Sequenced Distance Vector protocol (DSDV). Yang et al. [21] proposed identity – based broadcast encryption (IBBE) for efficient key management. The solution is lightweight and fast key agreement scheme. The scheme combines bilinear map and identity – based cryptosystem to achieve efficient group key agreement. The salient feature of the scheme is that member of a group has broadcasting capabilities. Each member will be able to find valid receivers and sends messages securely.

An anonymous secure routing using cryptography for MANETs was proposed by Aghaie and Adibnia [22]. The authors built a protocol to demonstrate the efficiency of the new security model they proposed. Their empirical results revealed that in the presence of latency the scheme achieved improved latency. In the presence of high traffic load, the scheme revealed significant improvement in data packet latency. Shobha and Jadhav [23] studied security problems in networks and proposed a scheme for secure communication in wireless networks. From the simulation experiments the scheme is proved to be effective as it could improve throughput besides being cost effective. Labbai and Rajani [24] proposed a secure group key management protocol that is based on message authentication code. The proposed scheme is named as variable bit rate on-demand routing protocol (VBOR). The message authentication code works in such a way that it does not allow malicious nodes to get messages. Only group members who know
A Review on Efficient Key Management Schemes for Secure Routing in Mobile Ad hoc Networks

MAC value can get messages. Residual energy of the nodes is considered for making this scheme to ensure the proposed scheme is energy efficient.

Pandya and Srivastava [25] studied the AODV protocol and made an extension to it. With this they concluded that the key management schemes can be avoided by extending AODV protocol efficiently. The reason behind is that the AODV is a popular routing protocol for mobile networks and that can accommodate more secure communication with some changes. Digital signature and secure hash algorithm are the two techniques used to improve security with AODV. Devaraju and Ganapathi [26] proposed a QoS based secure multicast key distribution in MANETs. A dynamic clustering approach is followed in order to achieve this. The methodology used to distribute key includes DSDV [27] and OMCT integration, then enhancing the integration, MDSDV [28] and CBMT, and efficient CBMT. The authors focused on phase 4 and achieved reduction of packet drop rate, end to end delay besides improving key delivery ratio and reduction of energy consumption. Sanghavi and Tada [29] proposed cluster based topology based secure key distribution scheme which is based on cryptographic function and network coding approaches. This scheme is secure and robust which incurs less communication cost. Zhu et al. [30] proposed an efficient group key management scheme named “GKMPAN” which will improve scalability, efficiency, and partially stateless.

[3] DISCUSSION OF SCHEMES

The PKI based scheme proposed by Capkun et al. [18] avoids the usage of CA and third party. Instead they use self-singed certificates. For room meeting scenarios the suitable key management scheme is the one proposed by which makes use of a common password. Instead of using the password directly, it is derived from a secret key. This provision is for preventing brute force attacks. It also exhibits two party key exchange and group key exchange. For master slave relationships proposed a scheme in which the master nodes exchange shared keys to slave nodes then the slaves use common secret key to authenticate master node. Thus the communication takes place securely. When all the participants are in the same physical space, the scheme proposed by is suitable. In this approach a MAC is attached to each packet by the sender. The receiver waits until all packets are buffered. Then the receiver takes the key disclosed by the sender thus it reduces one MAC operation for each outgoing packet. For reliable communication almost all schemes use pre-established key management schemes. Presented a scheme suitable for military operations. For complete security it does not use a single CA. Instead it makes use of multiple replicated CAs at various nodes arbitrarily. It can tolerate up to t compromised CA nodes. This is because it needs t+1 partial signatures are required in order to break it. Two protocols are used by the scheme proposed by Yuh-Min Tseng [17] for ensuring security in MANET. Collaborative key generation is used by in their scheme. It is a threshold public key management scheme. Cho et al. [15] used TSS for Cryptographically Generated Addresses (CGA) that ensures unbreakable security in MANET. The scheme of cluster based and provides efficient, fault tolerant and expandable key management scheme. Table 1 summarizes all the key management schemes applied for MANETs.
<table>
<thead>
<tr>
<th>Authors</th>
<th>Key Management Scheme</th>
<th>Techniques</th>
<th>Advantages</th>
<th>Limitations</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tseng [17]</td>
<td>heterogeneous-network aided public-key management scheme</td>
<td>Secure certificate distribution, symmetric secret key</td>
<td>Improving security infrastructure of public key management scheme, node identity confirmation</td>
<td>N/A</td>
<td>Wide-covered heterogeneous Networks are used for experiments</td>
</tr>
<tr>
<td>Hai-tao[14]</td>
<td>Cluster – based key management scheme</td>
<td>Id-based and hierarchical group key management</td>
<td>Secure, fault – tolerant, expansive, and efficient, delay rekeying policy</td>
<td>N/A</td>
<td>A MANET is considered for experiments where nodes are assumed to be roaming from one sub group to another sub group</td>
</tr>
<tr>
<td>Cho et al. [15]</td>
<td>Threshold secret sharing (TSS)</td>
<td>Cryptographically Generated Address (CGA)</td>
<td>More security</td>
<td>The proposed mechanisms were not evaluated.</td>
<td>Security is achieved in MANET without having a central CA</td>
</tr>
<tr>
<td>Cardone et al. [6]</td>
<td>Reliable communication for MANET-WSN scenarios</td>
<td>LQI link quality assessment</td>
<td>Effectiveness in providing security under mobility and challenging channel contention</td>
<td>Experiments are made over large scale deployments of MANETs</td>
<td></td>
</tr>
<tr>
<td>Devaraju and Ganapathi [26]</td>
<td>QoS based secure multicast key distribution</td>
<td>Dynamic clustering approach</td>
<td>Better QoS performance in terms of packet loss rate, key delivery ratio, energy consumption and end-to-end delay</td>
<td>N/A</td>
<td>NS2 version ns-allinone-2.33 was used to perform simulations</td>
</tr>
<tr>
<td>Sanghavi</td>
<td>Cluster based</td>
<td>Cryptographic</td>
<td>Prevention of Reliability of key</td>
<td>Experiments are</td>
<td></td>
</tr>
</tbody>
</table>
A Review on Efficient Key Management Schemes for Secure Routing in Mobile Ad hoc Networks

<table>
<thead>
<tr>
<th>Authors</th>
<th>Methodology</th>
<th>Key Management Scheme</th>
<th>Security Features</th>
<th>Issues</th>
<th>Topology</th>
</tr>
</thead>
<tbody>
<tr>
<td>C.Krishna Priya and Prof.B.Satyanarayana</td>
<td>Topology based secure key distribution</td>
<td>Method and network coding approach</td>
<td>Impersonation attacks, eavesdropping, authentication and confidentiality, less communication overhead</td>
<td>Distribution has not been evaluated</td>
<td>Made in cluster-based ad hoc hierarchical network topology</td>
</tr>
<tr>
<td>Deng, Mukharji and Agarwal [16]</td>
<td>Threshold and identity based key management</td>
<td>Distributed key management and authentication</td>
<td>Saves network bandwidth, and computational power besides providing end-to-end confidentiality and authenticity</td>
<td>N/A</td>
<td>Distributed key generation and identity based authentication is the two important features of the research.</td>
</tr>
<tr>
<td>Zhu et al. [30]</td>
<td>GKMPAN</td>
<td>Probabilistic key sharing scheme.</td>
<td>Efficiency, scalability (with less revoked nodes), and partially stateless</td>
<td>It has scalability problem especially when number of revoked nodes exist</td>
<td>It is a group key management protocol evaluated in MANETs.</td>
</tr>
</tbody>
</table>

Table 1 – Summary of key management schemes for MANETs

[4] CONCLUSIONS

In this paper we studied key management schemes in MANET that provide secure key exchange for reliable communication among the nodes which are vulnerable to various kinds of attacks such as location disclosure, black hole, replay, work hole, blackmail, denial of service and routing table poisoning. As the usage of MANETs became ubiquitous, it is essential to have complete security scheme in place to secure sensitive communications over MANET. As every node in the MANET is also responsible to cooperate in communications they are targets to attackers who launch attacks. The technical knowhow about various existing key management schemes can help in securing MANETs efficiently. In this paper we discussed various key management schemes found in the literature. This paper also throws light into various routing protocols and security challenges at various layers of protocol stacks.
REFERENCES


A Review on Efficient Key Management Schemes for Secure Routing in Mobile Ad hoc Networks


