Key Management for Group Based Mobile Ad Hoc Networks

Kamal Kumar Chauhan[1] and Amit Kumar Singh Sanger[2]

[1] Anand Engineering College, Agra, India
[2] Hindustan College of Science and Technology, Mathura, India
{kamalchauhans,sanger.amit}@gmail.com

Abstract. Security of a network depends on reliable key management systems that generate and distribute keys between communicating parties in network. Due to lack of central server and infrastructure in mobile ad hoc networks, this is a major problem to manage the keys in the network. Dynamically changes in network's topology causes weak trust relationship among the nodes in the network. In this paper, we proposed a key management scheme for group based mobile ad hoc networks, where a group leader has responsibility of key management in its group. Proposed key management scheme is a decentralized scheme that does not require any Trusted Third Party (TTP) for key management. Proposed key management system authenticates new node before joining the network and update the keys when a node left the network.

Keywords: MANET, Group, Key management, Authentication.

1 Introduction

A mobile ad hoc network (MANET) is a special type of wireless network in which mobile hosts are connected by wireless interfaces forming a temporary network without any fixed infrastructure. In MANET, nodes communicate each other by forming a multi-hop radio network. Mobile nodes operate as not only end terminal but also as an intermediate router. Data packets sent by a source node can reach to destination node via a number of hops. Thus multi-hop scenario occurs in communication and the success of this communication depends on other nodes' cooperation.

Security of a network is an important factor that must be considered in constructing the network. A network has to achieve security requirements in terms of authentication, confidentiality, integrity, availability and non repudiation. These security requirements rely on the availability of secure key management. Fundamental goal of a key management system is to issue the keys to the nodes in the network to encrypt messages, to manage these keys and to prevent the improper use of legally issued keys. Absence of key management makes a network vulnerable to several attacks [6]. Therefore, key management system is the basic and important need for the security of a network. A key management system normally involves key generation, distribution, updation and revocation of keys in network. The feature of MANETs

N. Meghanathan et al. (Eds.): CCSIT 2012, Part III, LNICST 86, pp. 455–464, 2012.

such as dynamic topology, lack of centralized authority, resource constrained and node mobility are the major challenge in establishment of key management. Some techniques such as intrusion detection mechanism consume lot of nodes' battery power but cannot account for flexible membership changes. However, an efficient and secure key management system can solve this problem with an affordable cost.

In this paper, we proposed a key management scheme for group based MANET where only group leader can generate, distribute, update and revoke keys in its group. Proposed key management scheme neither depends on a central server nor is it fully distributed. Our key management scheme is decentralized scheme that combines both centralized key management as well as distributed key management so that it can have the merits of both methods. On the other hand, proposed key management scheme is a hybrid key management scheme combining both Symmetric Key Cryptography (SKC) and Public Key Cryptography (PKC).

Rest of the paper is organized as follows. In section 2 some of the related work to key management scheme is discussed. The proposed key management scheme and group formation algorithm are presented in section 3. Security analysis of proposed solution is explained in section 4 and section 5 gives conclusions.

2 Related Work

Many of the key management schemes have been proposed for mobile ad hoc network. Some of the research papers which focus on key management in MANET are discussed below:

L. Zhou and Z. J. Haas [1] presented a secure key management scheme based on *(t, n)* threshold cryptography. The system can tolerate *t -1* compromised servers and this scheme does not describe how a node can contact *t* servers securely when server nodes are scattered in a large area and minimum *t* number of servers nodes have to present on ground every time, otherwise a new node cannot join network.

R. Blom [7] proposed a distributed symmetric key generation system based on the pre-shared keys and central server. Drawback of this scheme is that a node can derive the future key from the key chain which they have received from the main server and decrypt future traffic, hence lack of backward secrecy. Another problem is single point of failure.

H. N. Nguyen, H. Morino [8] proposed a threshold cryptography based scheme suited for MANET to provide robustness and defense against single point of failure. But main drawback in threshold cryptography is the difficulty in applying the distributive function. Drawback of this scheme is same as key management scheme proposed in [1].

L. Zhu, Y. Zhang, L. Feng [9] proposed a distributed key management scheme based on mobile agent carrying secret key and network state information. Limitation of the scheme is that it requires minimum *t* nodes must be present always to reconstruct the master private key. Another drawback is that continuously navigation of agent increases traffic and causes congestion in the network.

On the other hand, in the distributed certificate authority [3], [4], and [5] the authoritative power is distributed to several nodes. Since, it addresses the problem of single point failure. However, the major drawback is that the servers have to be chosen and pre-configured by an offline trusted party in advance. Another drawback of DCA is that the sufficient numbers of servers have to be present on ground.

3 Proposed Solution

3.1 System Model

A system model of open MANET is shown in Fig.1. Mobile nodes are divided into several groups in such a way that all the nodes are covered with no groups overlapped. Some of the nodes are selected as group leaders to perform key management and other administrative functions in its group. Aim of constructing the grouped based structure is that grouping in the network preserves the structure of network as much as possible, when nodes moves or topology is slowly changing. On the other hand, grouping reduces the number of keys, required for secure communication in network.

Group based structure divides the functions of a central server into several nodes (group leaders). Therefore, it combines both centralized and distributed approaches of key management providing decentralized solution. Such a structure of networks removes the vulnerability of compromising single central server. In the group based structure, if a group leader is compromised, only nodes of that group will be compromised and rest of the network will remain safe.

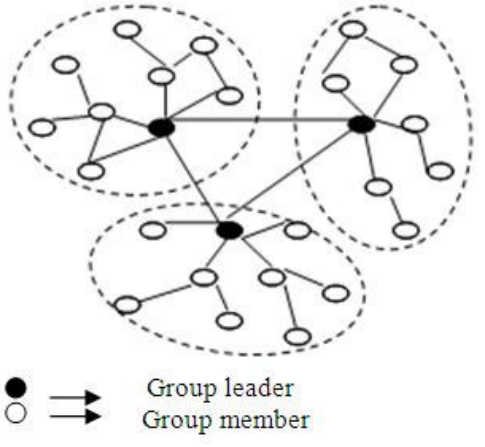

Fig. 1. System model for MANET

3.2 Group Formation Algorithm

Grouping or clustering is a process that divides the network into interconnected substructure known as groups. Grouping provides a better solution to the problem of key management and routing in MANET. But node mobility is major challenge for grouping in MANET. There is a group leader as coordinator in every group. Each group leader acts as a temporary base station within its zone or group and communicates with other group leader. A good grouping algorithm is one that divides the network into group in such this way that it preserves the structure of network as much as possible.

To select well suited node as group leader, we take into account its mobility, battery power and behavior of node. The following features are considered for grouping:

- Each group leader is capable to only support maximum 'x' number of nodes (a pre-defined value) efficiently. If a group leader is trying to serve more than 'x' number of nodes, the system's efficiency suffers.
- 'Mobility' is the important factor in deciding the group leader. Group leaders are responsible to preserve the structure of group as much as possible when nodes move or topology changing. Moving group leader quickly results detachment of nodes from group leader and also increases the probability of nodes' compromised. Mobility of a node is denoted by 'M' and can be measured as:

$$M = \frac{1}{T}\sum_{t=1}^{T}\sqrt{(Xt - Xt-1)^2 + (Yt - Yt-1)^2}$$

Where, (Xt, Yt) and (Xt-1, Yt-1) are the coordinates of a node at time t and t-1.

- 'Battery power' (B) is another important factor to decide a group leader. A group leader consumes more battery power than an ordinary node because a group leader has some extra responsibilities to carry out for its members. A node with maximum battery power should be selected as group leader.
- Another important parameter for electing the group leader is 'behavior of node'. A group leader is responsible for security of whole group. Group Leader monitors the nodes' activities continuously in the group and assigns them a Trust Level (T) on the basis of their behavior.

Finally, group leader is selected on the basis of weight (W), is defined as:

$$W = w_0M + w_1B + w_2T \quad (1)$$

where, w_0, w_1, and w_2 are the weight factor such as:

$$w_0 + w_1 + w_2 = 1 \quad (2)$$

Select a node as group leader with the smallest weight. All the neighbors of the selected group leader are no longer allowed to participate in the election procedure of group leader.

3.3 Key Management Scheme

In this section, proposed key management scheme in group based mobile ad hoc networks is described. Proposed key management scheme includes key generation, distribution and revocation phase. We make following assumptions:

- An offline Trusted Authority is available outside the network which is responsible only to issue a certificate and public/private key pair for the new joining mobile nodes.
- Intergroup communication is done through group leaders.
- Group leaders are trusted.

3.3.1 Key Generation and Distribution

All the group leaders in network are assigned a unique id. Each group leader has a public/private key pair and a secure hash function (e.g. SHA or MD5). We define three types of keys in the network: Group key, this is a common key for all the members in group used to encrypt/decrypt all the traffic communicated in the group. Second key, is a symmetrical key shared between group leader and a member node and third key, is shared among the group leaders in network.

Group leaders generate group key for their groups independently. Group key is updated each time when a node joins or leaves the group to maintain the forward and backward secrecy. Second key (k) shared between group leader and a member node is the function of node_id and a secret number (selected by and known only to group leader).

$$f(node\_id, Sr) = k \tag{3}$$

where f is a secure hash function selected by group leader , node_id is the id of node for which key 'k' is being generated and Sr is a secret number randomly selected by group leader and independent of the node_id.

Third key is shared among the group leaders in network. Group leaders can agree on a key to communicate securely using group Diffie-Hellman key agreement protocol [13]. This key is updated when a group leader is changed in any group and new elected group leader starts Diffie-Hellman key agreement to update the key.

3.3.2 Node Addition

Whenever, a new node wants to join the group. It sends a join request to group leader but this request might be captured by a malicious node in between group leader and new node to compromise the new node. On the other hand, a malicious node can also send a join request to group leader to join the group. Therefore, before joining the network it is necessary for both group leader as well as new node to authenticate each other. Upon successfully mutual authentication, a node can join the group and share a key with group leader in a secure manner. A new node can authenticate to group leader using challenge-response protocol. New node sends a challenge to group leader and group leader provide a valid response to be authenticated.

Group leader selects two large prime numbers 'p' and 'q' and calculates:

$$N=p*q$$

Group leader selects a random secret number 'S' and calculates:

$$V=S^2 \bmod N \qquad (1<S<N)$$

'N' and 'V' are publically announced in the group. When group leader has to authenticate itself i.e. it received a challenge from a node, it calculates:

$$X=R^2 \bmod N$$

where 'R' is a random number selected by group leader such that $1<R<N$.

Group leader sends {N, V, X} to new node as well as other members of group. After receiving (N, V, X), new node sends a challenge 'c' to all the members of group including group leader. Group leader calculates $Y=RS^C \bmod N$ and send it to

group members and new node. All the group members and the new node calculate XV^C and match with Y^2. If both values are same, group leader is successfully authenticated.

After successful authenticating to group leader, new node can sends its certificate to group leader which is encrypted with the private key of offline certificate issuer. Group leader verifies the certificate using public key of certificate issuer. If nodes' certificate is valid, group leader extracts the public key of new node from its certificate, generate a node_id and sends node_id and its public key to the new node encrypted with public key of new node. To make node_id unique across the network, group leader concatenates its id with node_id. Group leader generates a key using equation (3) and sends it to new node in secure manner. Group leader then update group key and group members list and sends to the members of group encrypting by previous group key and to new node encrypted by key shared between new node and group leader. After joining the network, new node broadcasts its id and public key in the group. When a new node joins the network, the communication between group leader and new node takes place as follows:

A group of mobile nodes with a group leader of MANET is shown in Fig.2, where a new node 'A' wants to join the group. Following are the notations used in communication:

$G \longrightarrow$ Group, {L, M}
$M \longrightarrow$ Set of group members $\{m_1, m_2, m_3 \ldots m_n\}$
$L \longrightarrow$ Group leader
$A \longrightarrow$ New node
$ID_A \longrightarrow$ A's Identity given by group leader
$K_{XY} \longrightarrow$ Session key shared between node X and Y
$e_X/d_X \longrightarrow$ Public key/Private key of node X
$DS_X \longrightarrow$ Digital Signature of node X
$T_X \longrightarrow$ Timestamp added by node X
$CERT_X \longrightarrow$ Certificate of node X
$S_{LX} \longrightarrow$ Symmetric key shared between group leader and node X.
X: Y $\{k(M)\} \longrightarrow$ Node X sends a message M encrypted with key k to node Y

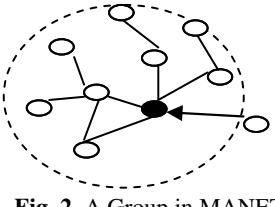

Fig. 2. A Group in MANET

A : L {A, Join_req}
L : A ∪ M {N, V, X}
A : L ∪ M {c}
L : A ∪ M {Y}

A : L {$CERT_A$}
L : A {e_A (e_L, ID_A, S_{LA})}
A : L {S_{LA} (num}
L : A {S_{LA} (num, member_list, group key)}
L : M {group_key (new_group_key)}

3.3.3 Key Agreement Protocol

If a node A wishes to communicate securely to node B. Before starting communication, they must agree on a session key. A starts communication by sending message:

$$A : B \{e_B (ID_A, ID_B, T_A, DS_A)\}$$

On receiving this message from A, B decrypts the message and verifies the signature of A using public key of A. If node B does not have A's public key, it sends a message to group leader conveying to send A's public key. Here following two cases are possible:

- A is a genuine node and group leader has pubic key of A. In this case, group leader sends A's public key to B. B then verifies A's signature and share a session key K_{AB}.

$$B : A \{e_A (ID_A, ID_B, T_A, T_B, DS_B)\}$$
$$A : B \{e_B (T_A, T_B, num1, K_{AB})\}$$
$$B : A \{K_{AB} (num1, num2)\}$$

- In second case, A is malicious node and not affiliated to group leader. In this case, group leader would inform to all the member of group that node A is not a member of group. It might be a malicious node.

3.3.4 Node Deletion

Whenever, a node leaves the group. Group leader removes that node from member list and intimate other member. Group leader regenerates new group key and sends other nodes in group, encrypted by the key shared with individual node. A node can be removed from member list when one of the following events occurs:

- A node can leave the group with prior notification.
- A node can leave the group without any prior notification or node is not forwarding the packets or performing as malicious node. Group leader exclude that node forcefully. In this case, group leader must inform to neighbor leader nodes.

On the other hand, when a group leader leaves the group with or without prior notification, a new group leader must be elected that can coordinate the group. New group leader reconstructs new group key and distributes it using unicast message encrypted with the public key of members and share a new symmetric key with each member in group. New group leader distributes its public key and id to other group leader in network and starts Group Diffie-Hellman key agreement [13] to update key shared among the group leaders.

4 Security Analysis of Proposed Solution

In this section, we discuss the security analysis of proposed solution against different attacks.

4.1 Backward Secrecy

When a node leaves the network either group leader or member node, it should not be able decrypt the future encrypted traffic. In proposed solution, when a member node leaves the group, group leader regenerates new group key and sends to members in group in a secure manner. On the other hand, when a group leader leaves the network, a new group leader is elected and it regenerates group key and distributes in its group in a secure manner. New group leader also starts Group Diffie-Hellman key agreement to update the key shared among group leaders. This ensures that keys are updated securely and backward secrecy is maintained.

4.2 Forward Secrecy

Forward secrecy says that when a new node joins the network, it should not be able to decrypt the past encrypted traffic. On joining of new node, group leader regenerates new group key and sends to members of group encrypted with old group key and unicasts to new node encrypted with key shared between group leader and new node, ensuring forward secrecy.

4.3 Mutual Authentication

In proposed solution, at the time when a new node joins the network both new node and group leader authenticate each other mutually. After successful mutual authentication, a new node can join the network. On the other hand, when two nodes wish to communicate, they also authenticate each other by sending their Digital Signature.

4.4 Man in Middle Attack

In Man in the Middle (MITM) attack, an attacker remains invisible between two nodes say A and B. Attacker splits the connection into two connections, one between node A and attacker and second, between attacker and second node B. Key management scheme proposed in [12] is vulnerable to MITM attack. In their solution, initiator (new joining node) sends its public key to receiver (central node). In response, receiver generates a session key and sends to initiator. This session key is encrypted with initiator's public key. In this scheme, if there is an attacker in between initiator and central node, attacker can capture the public key of new node and send its public key to central node. Then central node would share the session key with attacker and attacker shares session key with initiator. But in proposed solution, when a new joins the network first, it authenticates group leader using challenge-response protocol before sending its

certificate. An attacker cannot compromise a new node because challenge value from new node and response of the challenge from group leader are also sent to other members of group. In worst case, attacker can compromise the new node if and only if attacker had compromised all its neighbors already.

5 Conclusions

In this paper, we proposed a group formation algorithm and a key management scheme for group based mobile ad hoc networks. We described a secure key management scheme for group based a mobile ad hoc network that does not rely on a centralized authority for generating and distributing keys. Group leaders generate, maintain, and distribute the keys in their groups in a secure manner. Challenge-response protocol allows a new incoming node to authenticate to group leader, then joins group.

Proposed solution is a decentralized scheme and hybrid solution combining both symmetric and asymmetric cryptography algorithms. Security analysis of proposed solution in section 4 shows that proposed key management maintains forward and backward secrecy and provides security against many attacks such as reply attack, man in the middle attack etc. Limitation of proposed solution is that key management is based on public key cryptography, so it consumes more battery power in comparison of other key management schemes.

References

1. Zhou, L., Haas, Z.J.: Securing ad hoc networks. IEEE Network 13(6), 24–30 (1999)
2. Ge, M., Lam, K.-Y.: Self-healing Key Management Service for Mobile Ad Hoc Networks. In: Proceeding of First International Conference on Ubiquitous and Future Networks (June 2009)
3. Yi, S., Kravets, R.: MOCA: Mobile Certificate Authority for Wireless Ad hoc networks. In: 2nd Annual PKI Research Workshop, PKI 2003 (2003)
4. Luo, H.Y., Kong, J.J., Zerfos, P., Lu, S.W., Zhang, L.X.: Ursa: Ubiquitous and robust access control for mobile ad hoc networks. IEEE/ACM Transactions on Networking 12(6), 1049–1063 (2004)
5. Al-Shurman, M., Yoo, S.-M., Kim, B.: Distributive Key Management for Mobile Ad Hoc Networks. In: International Conference on Multimedia and Ubiquitous Engineering, pp. 533–536 (2008)
6. Kettaf, N., Abouaissa, H., Lorenz, P.: An Efficient Heterogeneous Key Management approach For Secure Multicast Communication in Ad hoc networks. In: Telecommunication System, vol. 37, pp. 29–36. Springer, Heidelberg (2008)
7. Blom, R.: Optimal Class of Symmetric Key Generation Systems. In: Beth, T., Cot, N., Ingemarsson, I. (eds.) EUROCRYPT 1984. LNCS, vol. 209, pp. 335–338. Springer, Heidelberg (1985)
8. Nguyen, H.N., Morino, H.: A Key Management Scheme for Mobile Ad Hoc Networks Based on Threshold Cryptography for Providing Fast Authentication and Low Signaling Load. In: Enokido, T., Yan, L., Xiao, B., Kim, D.Y., Dai, Y.-S., Yang, L.T. (eds.) EUC-WS 2005. LNCS, vol. 3823, pp. 905–915. Springer, Heidelberg (2005)

9. Lina, Z., Yi, Z., Li, F.: Distributed Key Management in Ad hoc Network based on Mobile Agent. In: Proceeding of 2nd IEEE International Symposium on Intelligent Information Technology Application, vol. 1, pp. 600–604 (2008)
10. Safdar, G.A., McGrath, C., McLoone, M.: Limitations of Existing Wireless Networks Authentication and Key Management Techniques for MANETs. In: Proceeding of 7th IEEE International Symposium on Computer Networks, pp. 101–107 (2006)
11. Yang, Y.-T., Zeng, P., Fang, Y., Chi, Y.-P.: A Feasible Key Management Scheme in Ad hoc Network. In: 8th Conference on the International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), pp. 300–303 (2007)
12. Boukerche, A., Ren, Y.: The Design of a Secure Key Management System for Mobile Ad Hoc Networks. In: The 33rd IEEE Conference on Local Computer Networks, pp. 302–327 (October 2008)
13. Zou, X., Ramamurthy, B.: A Simple Group Diffie-Hellman Key Agreement Protocol Without Member Serialization. In: Zhang, J., He, J.-H., Fu, Y. (eds.) CIS 2004. LNCS, vol. 3314, pp. 725–731. Springer, Heidelberg (2004)