Key Management in Mobile ADHOC Networks

K. Kiranmai[1] and M.Vijay Kumar[2]
[1]Student, M.Tech. (DECS), Department of ECE, Gudlavalleru College of Engineering, Gudlavalleru
[2]Assistant Professor, Department of ECE, Gudlavalleru College of Engineering, Gudlavalleru

***Abstract* - Ad hoc networking is a wireless networking paradigm for self-organizing networks that until recently has mainly been associated with military battlefield networks. However, with the availability of wireless technologies such as Bluetooth and 802.11 and the development of the next generation networks, civilian applications that exploit the advantages of ad hoc networking are being envisioned. So far most of the research has been carried out to address the routing issues. Whereas other issues such as security, key management and network addressing have received considerably less attention and these issues need to be addressed before any successful applications will appear. In this paper, we propose a security model by implementing a simple authentication along with Key Management technique. It is observed that the proposed security concept may increase the level of confidence in this network.**

Keywords - MANETS, key management, authentication, QoS.

IJERT

1. INTRODUCTION

Mobile ad hoc networks are different from mobile wireless IP networks in that there are no base stations, wireless switches, and infrastructure services like naming, routing, certificate authorities, etc. Because mobile nodes join and leave the network dynamically, sometimes even without a notice, and move dynamically, network topology and administrative domain membership can change rapidly. Thus it is important to provide security services such as availability, confidentiality, authentication [1,2], access control, integrity, and non-repudiation. As in other networks, cryptography is the foundation for all network security services [3] in MANET, and key management is the major factor to guarantee a secure ad hoc network [4].

The lack of proper infrastructure and central authority in Ad hoc Networks has necessitated the need to provide strong Key Management techniques. Key Management is the secure administration of Keys. A number of Key Management schemes have been developed in order to ensure maximum security to the data. Among many schemes, Threshold cryptography is one, in which a certain minimum number of users need to give a valid key to perform cryptographic operation. The number depends on the discretion of the user. For example in a k-out-of-n threshold scheme, any set of k users can compute the function while any set of k-1 users cannot. For certain applications such as general transfer of information between departments in a company it is enough if a limited minimum give a valid key for access to the network but in other applications such as in military, a large majority of people should give a valid key in order to access the information. So the threshold depends on the application in which it is used. Another major challenge is to deliver reliable data transmission when some nodes may be compromised [6]. Attackers can disrupt data transmission and incur significant data loss by tampering with, fraudulently redirecting, or even dropping data traffic.

1.1 Group Formation

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. 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 system model of open MANET is shown in Figure 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 the functions of key management system and other administrative functions in its group. Aim of constructing the grouped based structure is that grouping preserves the structure of network as long as possible, when nodes moves or topology is slowly changing. On the other hand, grouping reduces the number of keys, required to distribute in network for secure communication.

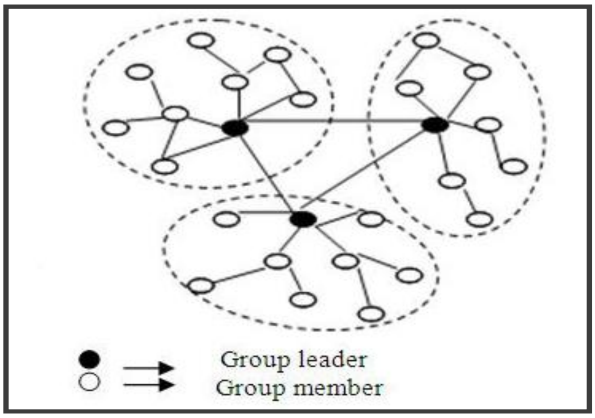

Fig. 1: System model for MANET

Group based structure distributes the functions of a central server into several nodes (group leaders). Therefore, it combines both centralized and distributed approaches of key management system providing a decentralized solution. Group based structure of networks also removes the vulnerability of compromising single

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

central server. If a group leader is compromised; only a group will be compromised leaving rest of the network safe and secure.

To select a well suited group leader, its mobility, battery power and behaviour of node is to be considered. The following features are considered for grouping:

- Each group leader is capable to support maximum 'x' number of nodes (a pre-defined value) efficiently. If a group leader is trying to serve more than 'x' nodes, 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. Moving group leader quickly results detachment of nodes from group leader and also increases the probability of nodes' compromised.
- '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 extra responsibilities such as monitoring group members and distribution of keys in the group. Therefore, node with maximum battery power should be elected as group leader.
- Another important parameter for electing the group leader is the 'behavior of node'. Security of a group is totally depends on group leader. Group Leader monitors the nodes' activities continuously in the group and assigns them a Trust Level (T) on the basis of their behavior.

Section 2 describes the security in Ad hoc Networks and section 3 describes proposed key management scheme. Section 4 describes the Simulation results and section 5 concludes.

2. SECURITY IN ADHOC NETWORKS

Ad hoc networks are a new wireless networking paradigm for mobile hosts. The military tactical and other security-sensitive operations are the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in design of these networks is their vulnerability to security attacks. Security is an important issue for ad hoc networks, especially for those security-sensitive applications.

2.1 Security Requirements

In order to analyze security (and security attacks) of a network, it is needed to define the requirements for a secure system. The basic requirements for a secure system are

- Confidentiality- only the intended receiver can access the information that is transmitted over the network
- Integrity- Integrity demands that everything is as it should be and that nothing should change.
- Availability- that a certain service should be accessible for an authorized user at any time and without unreasonable delay.
- Authenticity- that everyone can be proved (or disproved) to be the one they say they are.
- Accountability - keeping and protecting audit information so that the responsible party of any actions affecting security can be traced.
- Non-repudiation- the receiver and the sender of a message should not be able to later deny receiving or sending the message.

2.2 Security Attacks

All the basic security requirements described above can be attacked against. Attacks are either passive or active. The difference between these is that in passive attacks the attacker only collects the data passively, but in active attacks the attacker also uses the collected data for some malicious purpose. These include Eavesdropping, Traffic analysis Impersonation, Modification, Replay, and Denial of service.

3. PROPOSED KEY MANAGEMENT SCHEME

In this section, key management system is proposed for group based MANETs. Proposed key management scheme includes key generation, distribution and revocation phase. Whenever, a new node joins a group, it sends a request to group leader. This request might be captured by a malicious node showing as group leader to new node. Similarly, a malicious node can also send a request to group leader to join the group. Therefore, 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 and group leader can authenticate each other using challenge-response protocol. New node sends a challenge to group leader and group leader provide a valid response to prove its genuinity. To attain this, authentication protocols are needed with the objective that an authentication protocol should be lightweight and impose as small computational and message overhead as possible due to resources in a Mobile Ad hoc Networks are very limited.

Also, if the authentication protocol is very long-lasting it may requires huge memory and more power consumption. In our proposed method, a simple authentication protocol is implemented. Before sending a request to the group leader, the node in the network is required to append the one's complement of its own IP address and the node receiving the packet checks the authentication of its source by adding the appended one's complement. Any malicious node sneaking into the network does not know that it has to append the one's complement of its IP address and thus any packet from such nodes get dropped by its neighbours. Also, once a node fails the test for authenticity, a broadcast is made to the whole network, warning all the nodes in the network of the presence of a malicious node and its IP address. This saves processing time, as any node receiving any packet

IJERT

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

from the malicious node can simply discard it without any further checking. Thus the malicious node is isolated from the network. A group of mobile nodes with a group leader of MANET is shown in Figure.2, where a new node wants to join the group.

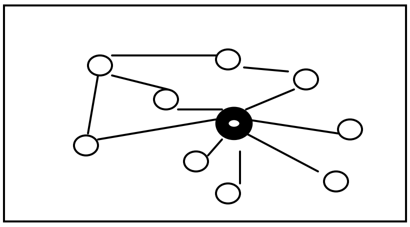

Fig. 2: A Group in MANET

3.1 Backward Secrecy

When a node leaves the network, it should not be able decrypt the future encrypted traffic. In proposed key management scheme, whenever a node leaves the group, group leader regenerates new group key and distribute it in the group. On the other hand, when a group leader leaves the network, a new group leader generates group key for the group. This ensures that keys are updated and backward secrecy is maintained in network.

3.2 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 generates 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.

IJERT

3.3 Mutual Authentication

In proposed key management system, both new node and group leader authenticate each other mutually at the time of network joining. After successful mutual authentication, node can join the network. When two nodes wish to communicate, they also authenticate each other by sending their Digital Signature.

3.4 Threshold Cryptography

Secret Sharing Schemes [5] allow for the division of keys so that an authorized set of users may access information. The idea of secret sharing is to start with a secret, divide it into pieces called shares, which are then distributed amongst users such that the pooled shares are specific subsets of users allowed to reconstruct the original secret. A secret sharing scheme where *k* out of *n* shareholders are needed to reconstruct the secret is referred to as a *(k, n)* threshold scheme.

3.4.1 Shamir's Secret Sharing

This *(k, n)* threshold secret sharing scheme proposed by Adi Shamir is based on polynomial interpolation and works as follows. The secret *S* is to be shared among the *n* shareholders identified by id_i, $i = 1... n$. The dealer who is the trusted party responsible for generating the secret and distributing it to the users performs the following steps:

- A prime *p* is chosen such that p>max(S,n)
- A polynomial

$$f(x) = a_0 + a_1 x + \ldots + a_k$$

is generated where a_0=S and a_i, i =1,…k-1 are chosen randomly from *Zp*.

- The shares *Si, i = 1,..., n* are generated as

$$S_i = f(id_i)\,(mod\,p)$$

- The shares are securely distributed to the respective shareholders.
- To reconstruct the secret Lagrange interpolation is used. With the knowledge of a minimum of *k* shares the polynomial *f(x)* can be reconstructed and the secret recovered by calculating *f(0)*.

The Lagrange interpolation is described below:

$$f(x) = \sum_{i=1}^{k} S_i \cdot l_{id_i}(x)\,(mod\,p) \;\text{ where }\; l_{id_i}(x) = \prod_{j=1,\, j\neq i}^{k} \frac{x - id_j}{id_i - id_j}$$

- It is important that no shareholder gains knowledge of any share other than his own. Otherwise he could potentially gain knowledge of *k* shares and then be able to reconstruct the secret himself.

4. RESULTS AND PERFORMANCE ANALYSIS

The proposed work is simulated and evaluated its performance using Glomosim simulator [6]. The following figures summarize the performance results with respect to various parameters obtained using GloMoSim by comparing with different speed and different number of nodes is presented.

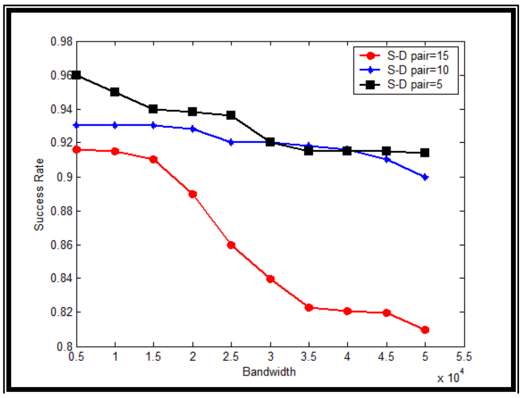

Fig.3 : Bandwidth Vs Success Rate

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

The success rate is defined as the ratio of the number of packets received successfully to the number of packets transmitted. The success rate is an important parameter to analyze the success of the routing scheme. Figure 3 shows the success rate versus the bandwidth. As the bandwidth increases, the numbers of packets received at the destination successfully are noted down. It is observed that as the demand on bandwidth increases the success rate decreases. The traffic rate is increased by increasing the number of source-destination pair. We have studied the simulation by varying the number of source-destination (S-D) pair as 5, 10 and 15 and it was observed that as the number of S-D pair increases the success rate decreases only by 4.2%. It was also observed that as the demand for bandwidth increases, the success rate decreases only by 3-6%. Hence it is concluded that an optimal success rate is obtained.

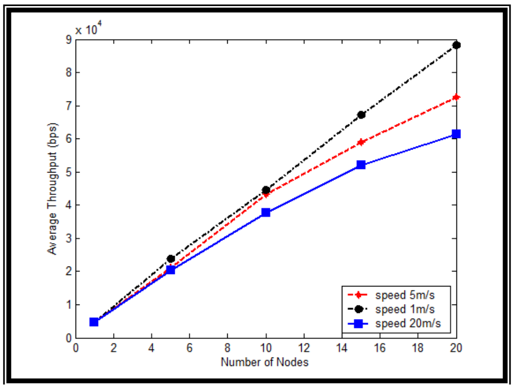

Fig. 4: Average Throughput Vs Number of Nodes

The Figure 4 presents the average throughput of network with different number of nodes and mobility. It has observed initially for smaller values of mobility, the increase in delay is not significant. So throughput is almost a constant and the average throughput is increased as the traffic in the network increases for less speed and decreases as the speed increases from 1m/s to 20m/s. Hence the average throughput decreases as the speed of the mobile increases.

IJERT

5. CONCLUSION & FUTURE WORK

Thus the proposed security scheme addressed simple authentication scheme and Threshold key management in mobile ad hoc networks in which, each user will have own Identity number and encrypted key. By utilizing digital signature, malicious alteration of data (i.e modification, insertion, deletion or replay) in transmission can be effectively protected. Our study concludes that the proposed security concept may increase the level of confidence in this network.

This work can be extended for implementing

- Power control protocols to reduce the power, which in turn increases the battery life.
- Image compression can also be implemented in Mobile Ad hoc Networks to save the bandwidth.
- Reduce Network contention
- QoS Topology Control in Ad Hoc Wireless Networks

REFERENCES

1. Prasant Mohapatra, Jian Li and Chao Gui, “QoS in Mobile Ad Hoc Networks”, Department of Computer Science, University of California, Davis, CA 95616, National Science Foundation Magazine, December 2002.
2. www.dspguide.com\datacomp.htm
3. William Stallings, ‘Cryptography and Network Security: Principles and Practice’, Second edition, 2001.
4. Helger Lipmaa, “Secret Sharing, Threshold Cryptography, MPC” Lecture notes in Cryptography and Data Security, T-79.159
5. Asokan N and Ginzboorg, “Key Agreement in Ad Hoc Networks”, Computer Communications,Volume 23, Pages 1627-1637
6. GloMoSim: Global Mobile Information Systems Simulation Library. http://pcl.cs.ucla.edu/projects/glomosim/.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)