Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 05, May-2016

Homogeneous Key Management Mechanism for Secure Group Communications in Manets

Inderpreet Kaur
Department of Computer Engineering
Mewar University
Chittorgarh, India

Dr. A. L. N Rao
Department of Computer Engineering
G.L Bajaj Engineering College Greater
Noida, U.P,

***Abstract*— The MANET (mobile adhoc network) creates a dynamic topology of networks than the traditional wired setup network. As a result network security is typical to manage in Manet. Scarcity of security makes Manet vulnerable to the attackers. The MANET suffers with various types of attacks that can come from any of the link which is in the range of Manet network. Denial of request, data tampering, message contamination, eavesdropping are some of the common MANET attack. Security of the MANET depends on the reliable management of cryptographic keys. Due to its dynamic topology it is tedious to maintain the key management of the network. In this paper we are proposing a scheme which will work on a trust management where the network is divided into different groups where the group leader of every group is shifting randomly. This group leader is responsible for generating secret public cryptographic keys. This method reduces the amount of keys to distribute among group members.**

Keywords*— *Cryptosystem, MANET, Key management , Public key

INTRODUCTION

A MANET is a self organising infrastructure network created by the mobile nodes itself. Maintaining a strong security for MANET is always a tedious task. Various research work has been proposed in past years for making a MANET a more secure network. For such type of network ,security is a challenging issue[1]. Dynamic topology and infrastructure less features makes it highly vulnerable to security. As these network requires all the security mechanism to be distributed . Due to these features it is difficult to implement security frameworks for MANET[2]

Traditionally Cryptographic systems are used to maintain data communication security. But if cryptographic system are deployed over MANET it does not provide the information about the reliability of the nodes[3]. However, key management [4,5] upto some extent is capable for maintaining a trust between the nodes but also lot of attention is required from security community due to the dynamic topology[6].

In this context trust can be defined as a procedure in which nodes without any previous interaction , establishes a trustworthy connection with a pre-exisiting level of trust among themselves[7]. To achieve a trust goal like authentication, integrity a secret key is required for the communication among the nodes in the network. But these keys has some limitation over MANET due to the high computational process. In this paper we have proposed a security extension to group based network working on security key management. We also proposed an algorithm to shared and exchanged a secret key between the group master and the group nodes during the creation of the group network of MANET.

Routing Protocols in MANET

Routing protocols in MANET are categorised as Proactive protocols, reactive protocols, hybrid protocols.

Proactive Protocols

These protocols demands each node in the network to maintain the tables by storing and updating the routing information and to acknowledge the other nodes within the network for the updation. These protocols works for optimum routes in terms of congestion and shortest path. Tables are updated at regular interval of time so that the tables should be synchronize. FSR, DSDV, OLSR[7] are few examples of proactive protocols.

Reactive routing protocol

These protocols are also known as on demand routing protocol. This protocol do not maintain routing table is there is no communication for establishing a proper connection with another node then the protocol sends a packet to another node then this protocol searches for the route in an on demand way and transmit and receive the packet . Such example is AODV[3].

Hybrid Protocols

Hybrid routing protocols works for high scalability over the network. It is because they minimises the number of rebroadcasting nodes and defines a well optimized network structure. ZRP[4] is use for high scalability and well optimized network over MANET.

Recent Work

Various security mechanism has been proposed for MANET. L.Zhou and Z.L.HaaS[8] has proposed a security key management framework. They proposed key function (k,n) of cryptography where n is the total nodes in the network and k are the nodes which will generate a secret key. And the network system can tolerate n-k dedicated servers. However this work has not explain clearly that how the node will contact to the servers as nothing is static in MANET and also there is no congestion control policy in the network where servers are communicating.

R.Blom[9] has proposed a distributed symmetric key generation system(SKGS). In this system a server is appointed for creation and distribution of keys in the network. But the demerit of the system is single point failure of the server. No further cryptographic keys will be given for the network.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 05, May-2016

Ngyen and Morino et.al[10] has proposed a system to overcome with the problem of single server failure. In this a central server for cryptographic key distribution allocates some group of servers . If any centralized server fails then any of the server among the group becomes a central server. But main drawback is applying the scheme over MANET because of its dynamic nature . And also to avoid congestion minimum server has to be in the network so that they can join other new node.

Yang Va-Tau.et.al[10] has proposed a scheme to create a group in MANET network. Key management is done in every group. In this scheme every group will have a group leader which will be responsible for key distribution in the same group. However this scheme does not describe the migration of group leader to another group. And also vulnerability of this scheme is that if the group leader fails due to several reasons the whole group will have to suffer.

In reference to [11] a scheme where distributed key will be managed by mobile agent is proposed. In this the mobile agent works as a central server and maintains the records of each and every node information by navigating itself. Demerit of this scheme is continuous navigating of mobile agent for updating will increase the problem of congestion in the network.

Proposed work

In this work we have proposed a security framework for MANET where we are dividing the whole network into several groups consisting of nodes and every group has a group master. The master will assign a unique id and a function to generate public and private key pair for itself and for the other nodes of network. In practical implementation we will assume the distance from master to the group member more than three hops.

To reduce the complexity of key distribution and the declaration of the group master dynamically without prior information of the existing master is the objective of the group based network.

Suppose there are m nodes in network and to share the public symmetric key the total number of keys will be

$$m(m-1)/3;$$

(considering three groups in the network)

So every node will have m-1 keys. If Public key cryptosystem(PKC) is applied , every node will save m+1 keys i.e m public and 1 private key. If we divide this into three groups key distribution will be in n/3 nodes and symmetric key will be evaluated as

$$\frac{(m/3(m/3-1))}{3}$$

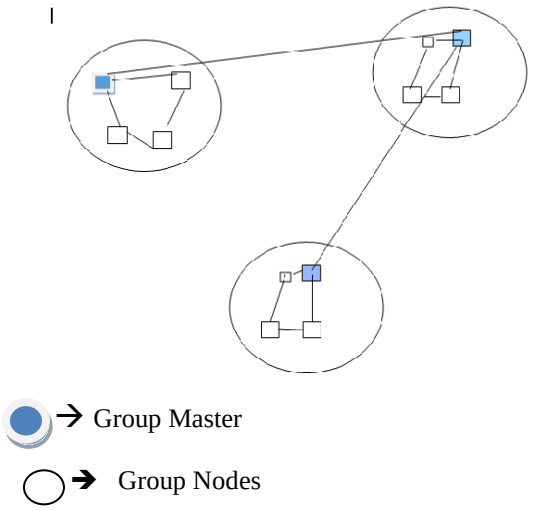

Fig 1 : System model of MANET

Key Management Policy

The key exchange policy of our proposed work works between the group leader and the group members.Here the group leader will have the following function for key exchange

Function1 (node_id, sizeof buffer,srv)

Size of buffer will hold m/3+1 keys.

Sr_v is the secret value known to the group master .

In our algorithm key exchange will work on two phases

1. Sharing the keys by the Group master to its group members
2. Sharing a secret key to the other groups masters

In this algorithm we are using symmetric key cryptography to establish a secure path between the group leaders and the group members. The group leader selects the private and the public keys for a secure communication.

Assume G is a group leader with a key generation function f(g). And g1,g2,g3…….g_n are the group nodes.

Here are the steps

Step 1- G chooses a large random number by using random function let say the number is x such that 0<x<n.
Step 2- g1,g2,g3…g_n also chooses a large random number using random function let say the number is Y such that 0<y<n.
Step 3- Let Say G send X to g1
Step 4- g1 sends Y to G.
Step 5- G calculates k=(X)xmod n
Step 6- g1 calculates k=(Y)mod n
Step 7- Values of keys should be same.
Step 8- Secure Connection Establish.
Step 8- g1 calculates k=(Y)mod n
Step 9- Values of keys should be same.
Step 10- Secure Connection Establish.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 05, May-2016

New Node Joining in the group
For each node in a network there are two types of cases
Case 1: If a new node wants to join the newly network and the group
Case 2: If an already existing node in the network wants to change its group

In first case if any node want to join any group in the network it will send a joining request to its neighbour member node then after receiving member node it will forward the request to the group master after the authentication. The group master will allot a secure public key and its group leader id to its newly node.

In Second Case
If existing node wants to change the group . The member node will share its node id ,public key and previous group member id to the new group leader. Now both the group leaders will check the validity of the existing member node.
For This case the notation are
G_1→ Group(L_1,g)
g→ group member (g_1,g_2,g_3.....g_n)
M→ group master
N→ new node
P_N→ Public key node of N
E_x(g)→ message encrypted key

Our Implementation Methodology

We are using C++ and NS2-2.35 simulator in ubuntu version 13.10 for implementing our proposed scheme. Steps are as follows

Step 1:- Setting parameters

Defining the variables for different layers working over manet like MAC, Buffer, Topology, Maximum packet transfer, routing protocol, number of mobile nodes setting up the group master using random function. Hash Function for encryption and propogation time

Step 2:- Defining the variables as global so that simulating trace file object.

Step 3- Defining the functions for each group and creation of mobile nodes.

Step 4- Generate the topology

Step 6- Assign the traffic pattern for the network

Step 7- Set the timer for start and stop for the simulator

Conclusion and Future Work
In this paper , we have proposed a secure key management mechanism by using the group based MANET where the groups master is completely responsible for generating and sharing of keys throughout the group nodes and other group masters of different groups. Here we have proposed the scheme to reduce the quantity of keys so that congestion overhead should be less and also proposed dynamically declaration of the group master without prior information by the existing group master so that the network should not be depended of some group masters for security. In our future work we will implement this proposed scheme .

REFERENCES

[1] Wu, B., Chen, J., Wu, J., Cardei, M.: A survey on attacks and countermeasures in mobile ad hoc networks, ch. 12, pp. 103–136. Springer, New York (2010)
[2] Zhou, L., Haas, Z.J.: Securing ad hoc networks. IEEE Network 13(6), 24–30 (2011)
[3] Li, X., Slay, J., Yu, S.: Evaluating trust in mobile ad hoc networks. In: Proceedings of the 2010 Workshop of International Conference on Computational Intelligence and Security, CIS 2005. Springer (2010)
[4] Lima, M.N., Pujolle, G., Silva, E., Santos, A.L., Albini, L.C.P.: Survivable keying for wireless ad hoc networks. In: Proceedings of the 2009 IFIP/IEEE International Symposium on Integrated Network Management (IM 2009), pp. 606–613. IEEE Communications Society (June 2009)
[5] apkun, S., Butty´an, L., Hubaux, J.P.: Self-organized public-key management for mobile ad hoc networks. IEEE Transactions on Mobile Computing 2(1), 52–64 (2012)
[6] P.S. Patheja , Akhilesh A. Waoo , Lokesh Malviya (2012) "Multipath Dynanic Source Routing Protocol for Ad-Hoc Network", International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 2, Issue 3, March 2012.
[7] Broch, J., Maltz, D., Johnson, D., Hu, Y., Jetcheva, J.: A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. In: Proc. ACM MobiCom 1998, pp. 85–97 (1998)
[8] L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network, vol. 13,no. 6,pp. 24-30, 1999.
I.-R. Chen, J.-H. Cho, and D.-C. Wang, "Performance Characteristics of Region-Based Group Key Management in Mobile Ad Hoc Networks," Proceedings of the IEEE International Conference on Sensor Networks, Vol. 1, pp. 411-419, June 2006.
[9] Yang Va-tao, Zeng Ping, and Fang Yong, Chi Ya-Ping., "A Feasible Key Management Scheme in Ad hoc Network", 8th ACIS Conference on the International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD),pp. 300, 2010.
[10] Merin Francis, M. Sangeetha and Dr. A. Sabari, "A Survey of Key Management Technique for Secure and Reliable Data Transmission in MANET", "International Journal of Advanced Research in Computer Science and Software Engineering", pp. 22-27 January – 2013.
[11] Wan AnXoing, Yao Huan Gong, "Secure and Highly Efficient Three Level Key Management Scheme for MANET", WSEAS TRANSACTIONS on COMPUTERS, Vol. 10, Issue 10, 2013.