

Securing Communication Over Co-Operative Remote Group In Manet

M.S. Antony Vigil

*Assistant Professor, Department of Computer Science and Engineering,
SRM University, Ramapuram, Chennai
Email id: antonyvigil@gmail.com*

S.Bagyalakshmi

*M.tech Student, Department of Computer Science and Engineering,
SRM University, Ramapuram, Chennai
Email id: bagyasankar@gmail.com*

R.Padmaja

*M.tech Student, Department of Computer Science and Engineering,
SRM University, Ramapuram, Chennai
Email id: padmaja234@gmail.com*

I. Abstract

Securing communication among co-operative remote group in MANET involves securing multicast group conversion in MANET. As the existing system proposes multicast key management system which involves a greater energy expenditure in terms of key distribution and updating, the proposed system introduces MESH based key management system. MESH based key management scheme delivers data of group conversion to all the participating nodes at same instant of time. It never forces the host of group conversation to stay online always. The simulation results prove that the proposed system perform well in terms of overhead and packet delivery than many other existing systems.

Index terms: Ad hoc networks, Manet, Information Security, Key Management

II. Introduction

MANET expanded as mobile ad hoc network is a self organizing network that connects mobiles through wireless infrastructures or without central server administration. An interesting point to note in MANET is there is no specific host or router or bridges involved, instead each mobile device is capable of acting as a host or a router in a multi-hop fashion. The application of MANET finds its large scope in the sectors where there is no possibility of establishing a network infrastructure (military battlefield, mining sectors, etc...)

MANET could be broadly classified into three based on its deployment environment. Layer oriented MANET is a network in which the trusted entities, hubs or special nodes exist and that is accessible from all nodes of the network. Flat oriented network is a network in which the trusted entities, hubs or special nodes exist but that remain not accessible from all nodes of the network. Military oriented MANET is a combination of above two frameworks.

Multicasting in MANET is a group oriented computing which promotes the transmission of datagram to group of hosts identified by a single destination address. Multicasting give rise to the concept of co-operative remote group through which the members of group can share the confidential information with high security. Multicasting allows the host to join or leave the group at any instant of time.

Multicasting suffers high security threats than unicasting as the data transmission occurs through multiple network channels. The most challenging threat that arises with multicasting is due to its adhoc nature of host to join or leave the group conversion instantly, hence establishing forward secrecy and backward secrecy becomes difficult.[Forward secrecy involves hiding the conversation that occurs after the host leaves the group. Backward secrecy involves hiding the conversation that occurs before the host joins the group.]

Key management is a process in MANET which performs creation, distribution and updating of keys for secure group communication. In group communication it becomes necessary to update the key immediately when a new host enters or the existing host leaves the conversation so as to ensure the forward and backward secrecy. The updating of key termed as re-keying tends to waste enormous amount of energy of network.

III. Related works

Due to various intrusion attacks and multichannel transmission vulnerable, it becomes inevitable to secure the transmission through key encryption. A central key encryption scheme is one of the scheme for securing multicasting which involves i. key pre-distribution involves distribution of keys to the node before deployment through which the node builds the network ii. Authenticated node revocation involves authenticating the node iii. Secure group key distribution involves safeguarding the process of key distribution iv. Key updating involves updating the key frequently. In Central Key encryption, all the key management operations are performed by Group controller whereas in distributed key encryption scheme is performed by the users themselves.

The research to secure communication among group of MANET started in the way back of 1980's which gave way to raise of various key management protocols. In early key distribution system, a trusted server creates and passes secret keys to the members of group conversation. On those days, the participants of group conversations seems to be static and remained similar to broadcast. A broadcast encryption technique is used in this conventional key distribution system. As the days passed, the count of participants of group conversion becomes ad hoc, which geared up the research towards key management scheme in a different angle giving rise to below inventions.

In two level hybrids MANET scheme, a core based tree key management protocol was implemented. The Member organization takes up a tree structure. The group members are always placed at leaf node and key is associated with the root node. Each member in the group knows all key from its leaf node up to root. But CBT key Management protocol suffered a serious advantage based on the fact A node can have any no. of children nodes hence sibling nodes can identify the keys of each other.

Following the drawbacks of CBT protocol, Group Key Management Protocol (GKMP) comes into the existence. In GKMP, a single node acts as a GSA (Group Security Agent) which distributes individual and session key to the group members. But Multicasting fails badly, when GSA becomes a faulty node or node out of reach.

Later, one way function tree protocol (OFT) an enhancement of CBT protocol comes into the existence, rectifying the bugs of CBT protocol. One way function tree protocol proposes that an interior node can have only two leaves. Each member knows the un-blinded node keys on the path from its node to the root and the blinded nodes are the siblings to the nodes in its path to the root.

Following TGDH (Tree Group DH) was introduced, it differs from OFT in one aspect that any node can act as a leader depending upon its position in tree, a member knows all blinded keys of tree at any given time and the merging function is two-party DH key exchange.

The research work of Fast transmission to remote cooperative groups proposes a new key management paradigm combining the techniques of broadcast encryption and group key agreement. But it fails miserably as the effort and cost involved in key management become enormous when host is added or deleted from the group.

My research work "Securing communication among co-operative remote group in MANET" proposes two level hybrid MANET network and Mesh based Key management technique to enhance the multicast communication with less effort and minimum budget.

IV. System Architecture

Securing communication among co-operative remote group in MANET builds a two level hybrid model network in which GSC and GSAs play a crucial role. GSC expanded as Global Security Controller heads the whole network, performs Traffic key encryption authenticates each node before it enters the MANET. GSC controls GSAs which is capable of performing multicasting within the remote groups.

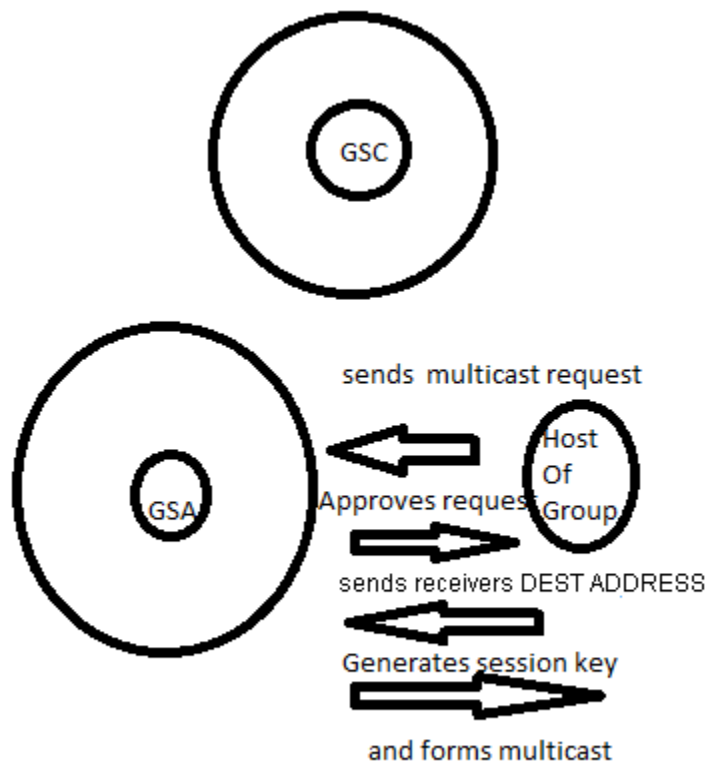


Fig 2: GSA processing Multicast Request

Member’s organization inside group

GSA organizes the members of group in the form of MESH MANET in which each node is connected to its neighbor as well with GSA. Mesh based configuration makes the key distribution easier.

Each node transfers its message to GSA, encrypting it with its traffic key and session key. GSA decrypts it and then transfers it to other participant nodes.

Re-keying inside group

GSA keeps monitoring the participants of group conversation, when it feels a participant is inactive for a fixed time, it seeks the approval of the host of group deletes destination address of the inactive node, marking it as a user left the conversation and regenerates the session alert for group members.

It is very interesting to note GSA distributes session key only at first instance, from second instance it just sends a signal based on which all other participant nodes calculates the session key. Car Michael Function has been used by the group participant nodes to calculate the session key.

Carmichael function of a positive integer n , denoted $\lambda(n)$, is defined as the smallest positive integer m such that

$$a^m \equiv 1 \pmod{n}$$

for every integer a that is coprime to n . Initial Session key value of each node act as the value of n .

When an inactive participant node is to be removed, GSA does not signal it for new session key generation and when the session key changes, the inactive participant node moves out of the conversation.

When GSA gets a new member addition request from the host of the group conversation, GSA places new node between the last node and first node of MESH MANET, hence the problem of addition or deletion of member into a group conversation becomes much easier. Each time it is responsibility of GSA to create a unique session key for newly added participant node.

MESH based Key Management system allows both the data and key transmission to be synchronized.

Mesh based Key Distribution

The nodes of the mesh determine the number of mesh which in turn controls the number of GSA. The main idea of mesh based organization is to partition the nodes of multicast and group them based on the similarity.

The number of keys generated by GSA (denoted by S)

$$S = n * D_o + n * D_{in} + n$$

$$S = n (D_o + D_{in} + 1)$$

D_o = No. of Dial out in Multicast

D_{in} = No. of Dial-in in Multicast

At times, if more number of nodes do participate in multicast it becomes impossible for single GSA to host group chat. If the nodes of equal energy is participating in the multicast, the below

$$P_{GSA} = \sum (P_n)^N$$

$$\log P_{GSA} = N \log \sum (P_n)$$

$$N = \log P_{GSA} / \log \sum (P_n)$$

P_{GSA} - energy of GSA node

$\sum (P_n)$ – cumulative energy of nodes

N – decide no. of GSA

How GSA's communicate with each other

Since Intrusion could be done at any level, it is necessary to protect the communication between GSA as well. Hence message centric encryption scheme has been employed to secure the message at GSA level

Message centric encryption

GSA Sender receives MSG A

Perform LEN (MSG A)

Right shift each character of the message by LEN

Obtains encrypted MSG A
 Perform Send(MSG A)

Message centric decryption

GSA Receiver receives MSG A
 Perform LEN (MSG A)
 Left shift each character of the message by LEN
 Obtains decrypted MSG A

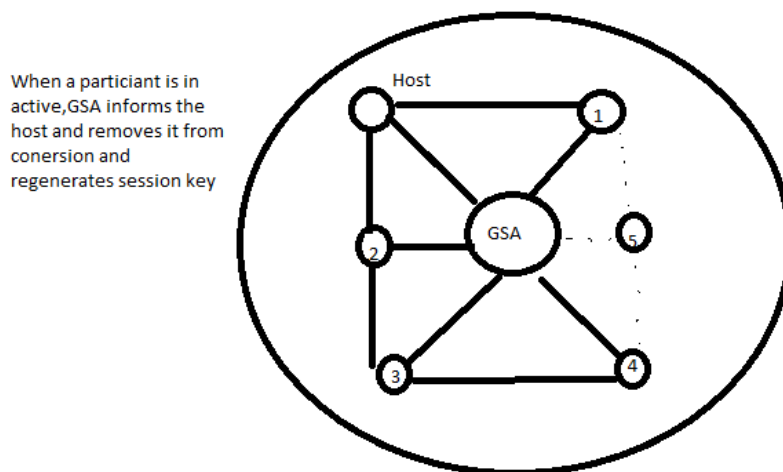


Fig 3: GSA removing an inactive Participant

Communication between GSC and GSA

There is a need to ensure the communication between GSC and GSA as there are wide open opportunities to make compromised node attacks by compromising GSA. Hence data communication between GSA and GSC are safeguarded by Common prime encryption scheme.

Encryption Common Prime Algorithm

GSC shares common prime number (p) and base number (g) to all GSA.

- GSA selects an integer a $A = g^a \text{ mod } (p-1)$ and passes A to GSC
- GSC selects an integer b $B = g^b \text{ mod } (p-1)$ and
- Passes B to GSC
- GSA calculates $\text{Key} = B^a \text{ mod } (p-1)$
- GSC calculates $\text{Key} = A^b \text{ mod } (p-1)$

Now both GSA and GSC shares same Key for encryption and decryption.

V. Experimental Setup

In demonstration experiment, I have employed NS2 simulators to simulate Securing communication among co-operative remote group in MANET. The channel capacity of our mobile host is fixed at 2Mbps. In order to employ multicasting among remote co-operative group have used multicast AODV routing protocol. This simulation model works on the assumption each mobile node moves independently with the same average speed.

Table 1: Simulation Parameters

No.of nodes	30
Area size	500X500
Simulation time	60Sec
Routing Protocol	MAODV
Transmit power	0.6w

VI. Performance Metrics

Comparing MESH key management with GKMP, The proposed system have considerable advantages in terms of packet delivery ratio, energy consumption and overheads. [Average Packet Delivery Ratio is the ratio of no. of packets sent and received. Average Energy Consumption is energy spent by a node in receiving and sending a node. Overhead is a measure of keying and re-keying.]

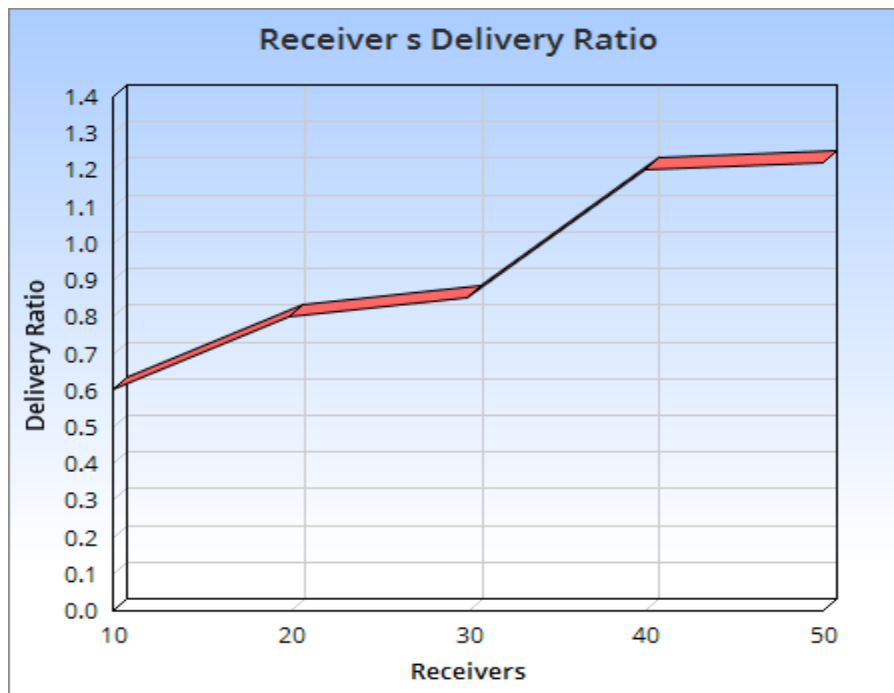


Fig 4: Graph depicting Delivery Ratio

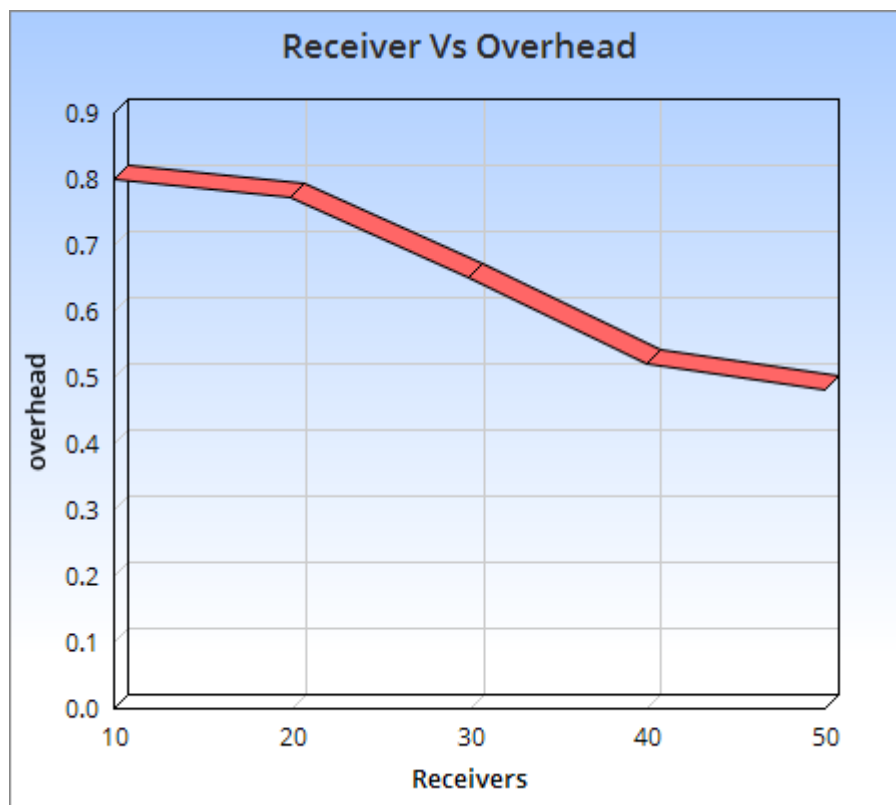


Fig 5: Graph depicting overhead of re-keying

VII. Conclusion

In this paper, I have proposed two level hybrids MANET network and MESH based Key management system for secure multicasting among remote groups. In further works, I would like to develop powerful encryption scheme that negotiates frequent re-keying that is required to maintain forward and backward secrecy in multicasting.

VIII. References

- [1] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.
- [2] M. Weiser, The Computer for the Twenty-First Century, Scientific American, September 1991.
- [3] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63–70, July-August 1999.
- [4] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

- [5] Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security, November/December 1999.
- [6] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.
- [7] Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 31), CRC Press LLC, 2003.
- [8] Yi-an Huang and Wenke Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks, in Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, Fairfax, Virginia, 2003, pp. 135 – 147.
- [9] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity.
- [10] P. Papadimitratos and Z. J. Hass, Secure Routing for Mobile Ad Hoc Networks, in Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, January 2002.
- [11] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02, 2002.
- [12] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks, in Proceedings of ICNP'02, 2002.
- [13] Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, Ad Hoc Networks, 1 (1): 175–192, July 2003.
- [14] Y. Hu, A. Perrig and D. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks, in Proceedings of IEEE INFOCOM'03, 2003.
- [15] Y. Hu, A. Perrig and D. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, in Proceedings of ACM MobiCom Workshop - WiSe'03, 2003.