ISSN - 2348-2397
APPROVED UGC CARE

SHODH SARITA
Vol. 7, Issue 26, April-June, 2020
Page Nos. 201-206

AN INTERNATIONAL BILINGUAL PEER REVIEWED REFEREED RESEARCH JOURNAL

# SECURE MULTICAST KEY DISTRIBUTION IN MANET USING CLUSTER BASED MULTICAST TREE

❒ Prof. Sagar Thakare*

## ABSTRACT

Wireless networks and network devices are popular as they provide users access to information and communication anytime anywhere. Conventional wireless communications are usually supported by a fixed infrastructure. A mobile device would use a single hop wireless communication to access a base station. But Ad Hoc Network is infrastructure-less. The nodes in an Ad hoc network communicate via single hop or multi-hop path in a peer-peer fashion. The proposed work is to build virtual clusters throughout the networks. Each cluster has a cluster head and the other nodes of the cluster are the member nodes. With the help of the cluster heads, the nodes authenticate each other and exchange their public key in a secure manner. The cluster head selection is based on the degree of nodes and node's ID identification number. Apart from these, parameters the member nodes assess trust of the cluster head. The main idea in this project proposal is Key Management for secure group communication in Ad Hoc Networks. Group communication is one of the most important services in a mobile Ad Hoc networks, in which data confidentiality and integrity is realized by encrypting data with cluster key (Group key). The proposed scheme in the project tries to achieve better scalability by cluster formation and regard to key management, the system tries to address the communication overhead and partial distribution in threshold key management scheme and improve the success rate in key management.

**Keywords :** Cluster based multicast tree, MDSDV, Mobile Adhoc Networks, Multicast Key Distribution

## Introduction

As the importance of computers in our daily life increases, it also sets new demands for connectivity. Wired solutions have been around for a long time but there is increasing demand on working wireless solutions for connecting the Internet, reading and sending E-mail messages, changing information in a meeting and so on. There are solutions to these needs, one being wireless local area network that is based on IEEE 802.11 [1] standard. However, there is increasing need for connectivity in situations where there is no base station (i.e. backbone connection) available (for example two or more PDAs need to be connected), there emerges Ad hoc networks.

The popular IEEE 802.11 "Wi-Fi" protocol is capable of providing Ad hoc network facilities at low level, when no access point is available. However in this case, the nodes are limited to send and receive information but do not route anything across the network. Mobile Ad hoc Networks can operate in a standalone fashion or could possibly be connected to a larger network such as the Internet.

Mobile Ad hoc Networks can turn the dream of getting connected "anywhere at any time" into reality. Typical application examples include a disaster recovery or a military operation. Not bound to specific situations, these networks may equally show better performance in other places. As an example, imagine a group of people with laptops, in a business meeting at a place where no example, imagine a group of people with laptops, in a

*Assistant Professor - NCRD's Sterling Institute of Management Studies, Nerul, Navi Mumbai

business meeting at a place where no network services is present. In such a situation their machines can form an Ad hoc network. This is one of the many examples where these networks may possibly be the best ones to cater the needs of dynamic nature.

A MANET (Mobile Ad Hoc Network) is an autonomous collection of mobile users that offers infrastructure-free architecture for communication over a shared wireless medium. It is formed spontaneously without any preplanning. Multicasting is a fundamental communication paradigm for group-oriented communications such as video conferencing, discussion forums, frequent stock updates, video on demand (VoD), pay per view programs, and advertising. The combination of an ad hoc environment with multicast services [2], [3] induces new challenges towards the security infrastructure. In order to secure multicast communication, security services such as authentication, data integrity, access control and group confidentiality are required. Among which group confidentiality is the most important.

**Mobile Ad hoc Networks (MANET)**

In recent years, Mobile Ad hoc Network (MANET) has received much attention due to self-design, self-maintenance, self-organized and cooperative environments. In MANET, all the nodes are mobile nodes and the topology will change rapidly without any predefined infrastructure. Participating nodes can be laptops, palmtops, cell phones etc. Each device can act both as a host and a router to forward packets for other nodes. The structure of the MANET [4] shown in Fig.

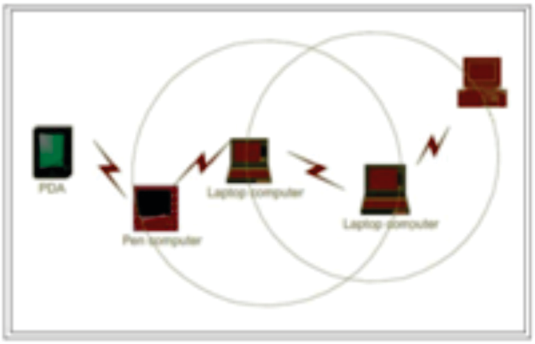

Figure 1: Structure of MANET

Here, the mobile devices such as PDAs and laptops are used to route the data packets. In MANET, all the nodes actively discover the topology and the messages are transmitted to the destination over multiple-hop. It uses the wireless channel and asynchronous data transmission through the multiple-hop. The vital characteristics of MANETs are lack of infrastructure, dynamic topology, multi-hop communication and distributed coordination among all the nodes [5],[6].

**Key Management Requirements**

In a secure multicast communication, each member holds a key to encrypt and decrypt the multicast data. When a member joins and leaves a group, the key has to be updated and distributed to all group members in order to meet the multicast key management requirements. Efficient key management protocols should be taken into consideration for miscellaneous requirements. Figure summarizes these requirements.

**Quality of service requirement**

**i. "1 affects n":** If a single membership changes in the group, it affects all the other group members. This happens typically when a single membership change occurs all group members commit to a new TEK.

**ii. Energy consumption:** This induces minimization in the number of transmissions in forwarding messages to all the group members.

**iii. End to end delay:** Many applications that are built over the multicast services are sensitive to average delay in key delivery. Therefore, any key distribution scheme should take this into consideration and hence minimize the impact of key distribution in the delay of key delivery.

**iv. Key Delivery Ratio:** This induces number of successful key transmission to all group members without any loss of packet during multicast key distribution.

Thus a QoS based secure multicast key distribution in mobile Ad hoc environment should focus on security, reliability and QoS characteristics.

To overcome these problems, several approaches propose a multicast group clustering . Clustering is dividing the multicast group into several sub-groups. Local Controller (LC) manages each subgroup, which is responsible for local key management within the cluster.

Thus, after Join or Leave procedures, only members within the concerned cluster are affected by rekeying process, and the local dynamics of a cluster does not affect the other clusters of the group and hence it overcomes “1 affects n” phenomenon. Moreover, few solutions for multicast clustering such as dynamic clustering did consider the QoS requirements to achieve an efficient key distribution process in Ad hoc environments.

## Literature Review

Key management approaches can be classified into three classes: centralized, distributed or decentralized. Figure illustrates this classification. In centralized approaches, a designated entity (e.g. the group leader or a key server) is responsible for calculation and distribution of the group key to all the participants. GKMP achieves an excellent result for storage at the members[2]. However, this result is achieved by providing no method for rekeying the group after a member has left, except re-creating the entire group which induces O(n) rekey message overhead where 'n' is the number of the remaining group members.

As per research, Integration of Optimized Multicast Tree with DSDV.The main idea of this integration is to integrate OMCT clustering algorithm with DSDV routing protocol to elect the local controllers of the created clusters[3]. The principle of this clustering scheme is to start with the group source GC, to collect its 1-hop neighbors by DSDV, and to elect LCs which are group members and which have child group members (the LC belongs to the unicast path between the source and the child group members).

When integrate Cluster Based Multicast Tree with MDSDV. Cluster based multicast tree (CBMT) with MDSDV algorithm is a new reliable version of OMCT with DSDV for secure multicast key distribution in mobile ad hoc networks. It includes key tree engine and forms tree structure based on authentication. Multicast version of DSDV routing protocol is used to form multicast tree among the group members. Thus this method proposes a reliable dynamic clustering approach by reducing the packet drop ratio and increasing the key delivery ratio. In many multicast interactions, due to its frequent node mobility, new members can join and current members can leave at a time[6]. The moving behavior of each member in the MANET should be realistic.

The problems of the membership dynamism can be overcome by using mobility aware MDSDV routing protocol. It allows fast reaction to topology changes and is specially designed for MANET. Hence, this proposes an Advanced CBMT with mobility aware MDSDV for secure multicast communication. It tolerates the faults that occur due to node failure. The proposal of this system is to present a new Advanced CBMT .It used for to tolerate the fault ,Improved the key delivery ratio, reduced end to end delay, less energy consumption, increased key delivery ratio, Reduced Packet Drop ratio[9].

## Proposed Methodology

### Advanced CBMT

Here Algorithm is proposed for this project and the main idea of Advanced CBMT is to use Mobility aware Multicast DSDV routing protocol to elect the local controllers of the created clusters by considering the node failure. The CBMT algorithm generates a cluster based multicast tree for secure communication. The principle of the proposed clustering approach is described in steps as follows.

### Advanced CBMT Algorithm

When All the group members covered by its clusters and the created clusters are not yet cover the group members and hence the nodes are selected as local controllers for the remaining group members.

Following steps applied when node is in Mobile, Load of the clusters are increases because of node increases and node failure in the cluster, not easy to elect new LC.

### Step-I

Traverse the formed cluster, due to membership dynamism, if a cluster has group members more than the maximum threshold, then split the cluster and elect the new LC based on the one hop distance reachability information.

### Step -II

Traverse the formed cluster, If the cluster has group members lower than the minimum threshold, then traverse the group members of this cluster and try to move them to the nearest cluster.

Thus the efficiency of CBMT approach is improved, while forming highly correlated clusters based on the two thresholds. Thus this approach is considered as an Advanced CBMT. The improvements in the advanced CBMT with mobility aware MDSDV approach for multicast key distribution are describe in Algorithm.

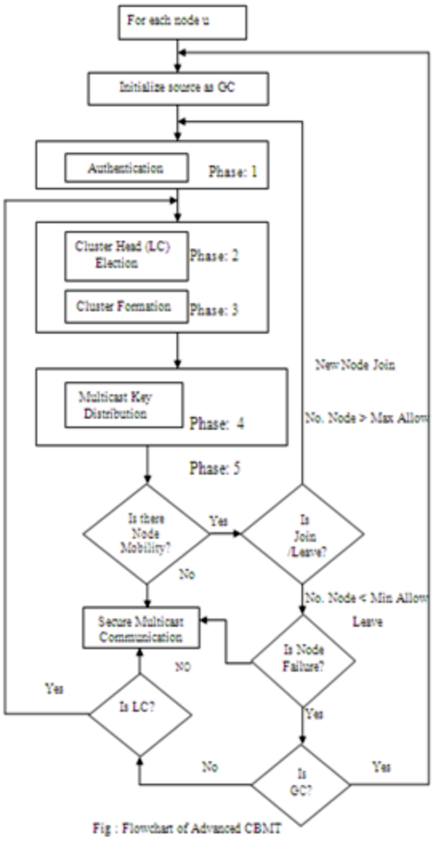

Fig : Flowchart of Advanced CBMT

## Performance Evaluation

The performance of proposed methodology for secure multicast key distribution is evaluated in terms of QoS metrics.

**Performance Metrics**

I have proposed to evaluate a following parameter by using CBMT with Mobility Aware MDSDV.

**1)** End to End delay in key distribution,

**2)** Energy consumption,

**3)** Key delivery ratio and

**4)** Packet drop ratio of multicast key distribution.

**5)** Fault tolerance.

**1)** **End to End Delay :** It indicates the average latency or end to end delay of key transmission from the source to the receivers. This metric allows evaluating the average delay to forward a key from a LC to its cluster members. Transmission delay is calculated as in eqn. (3.2),

$$TD(N) = t_s + t_k + \sum_{i=1}^{n} ((1 - pi)Ni)$$

N :-> No. of packets from source to destination

Ni :--> No. of packets transmitted to path pi--> packet drop ratio

TD :--> Transfer delay $t_s$--> setup time $t_k$-->key transmitting time

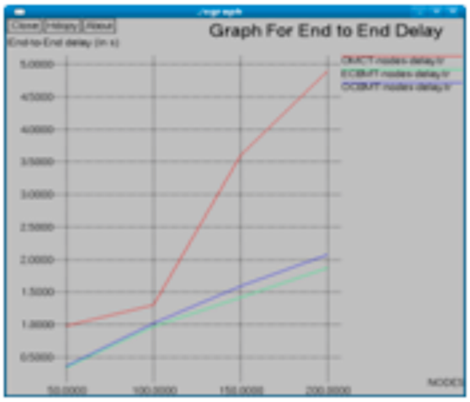

Fig: Output Graph for End to End Delay

**2)** **Energy Consumption** is defined as the sum of energy units required to the key transmission throughout the duration of multicast data transmission. This is illustrated with an example in a multicast tree as shown in the Figure.

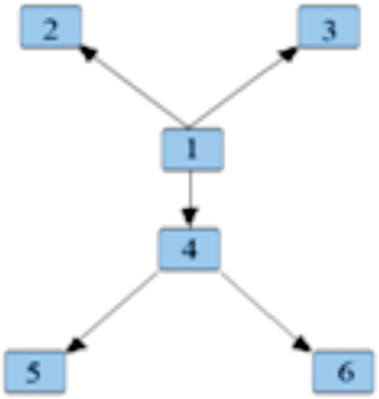

Figure 4.2 Energy consumption of multicast key distribution

$E_{MAX}$=MAX [[ $E_{1\text{-}2}$,$E_{1\text{-}3}$, $E_{1\text{-}4}$] ,[ $E_{4\text{-}5}$] ,[ $E_{4\text{-}6}$]]

$E_{MIN}$= MIN [[ $E_{1\text{-}2}$,$E_{1\text{-}3}$, $E_{1\text{-}4}$] ,[ $E_{4\text{-}5}$] ,[ $E_{4\text{-}6}$]]

$E_{TOT}$= [$E_{MAX+}E_{MIN]}$]

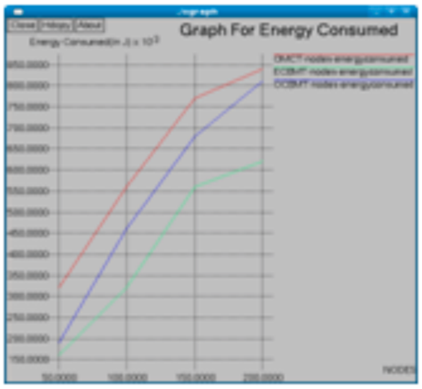

Fig: Graph for Energy consumption

3) **Key Delivery Ratio** is defined as the number of received keys divided by number of sent keys. This metric allows evaluating the reliability of the protocol in terms of key delivery ratio in key transmission from the source to the group members as in eqn.

$$\mathrm{KDR} = \frac{\text{number of received keys}}{\text{number of sent keys}}$$

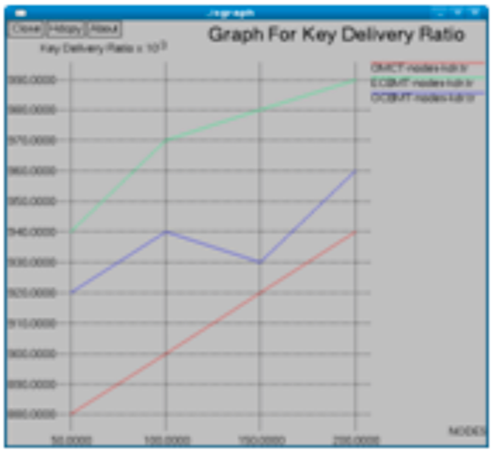

Fig : Graph for Key delivery ratio

4) **Packet Drop Ratio :** is the ratio between the number of packets received at the destination and the number of packets sent to the destination. This metric allows in evaluating the reliability of the protocol in terms of packet drop ratio in key transmission from the source to the group members as in eqn.

$$\mathrm{PDR} = \frac{\text{No of packets received at the destination}}{\text{No of packets sent at the destination}}$$

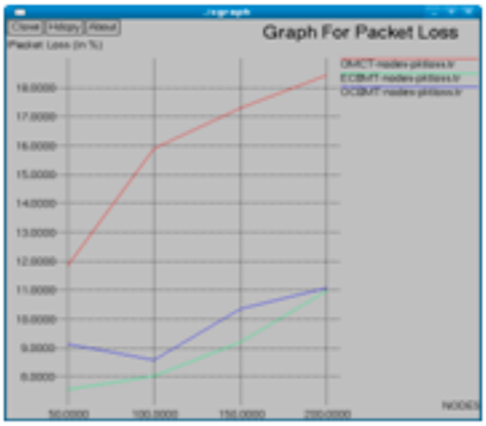

Fig: Graph for Packet drop ratio

5) **Fault Tolerance :** As number of nodes increases, it increases the fault-tolerance in key distribution. Indeed, this approach divides the multicast group with the effective connectivity between nodes. It allows fast reaction to topology changes. This is due to the fact that it sends acknowledgement for each transmission in order to reduce the retransmission. Hence it tolerates the fault that occurs due to node failure of multicast transmission in advanced CBMT compared to OMCT.

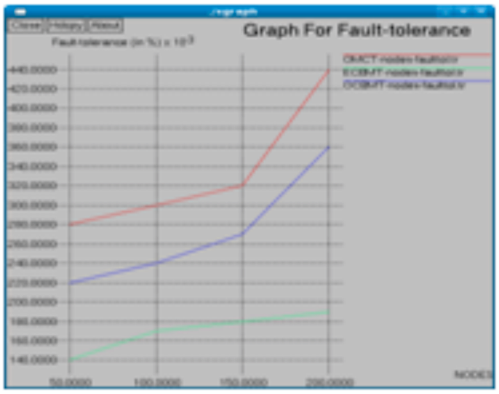

Fig: Graph for Fault tolerance

## Conclusion

Many emerging applications in Mobile Ad hoc Networks involve group oriented communication. Multicast is an efficient way of supporting group oriented applications, mainly in mobile environment with limited bandwidth and limited power. For using such applications in an adversarial environment as military, it is necessary to provide secure multicast communication.

Secure multicast communication in Mobile Ad hoc Networks is challenging due to its inherent QoS characteristics of infrastructure less architecture with lack of central authority, high packet drop ratios and limited resources. Hence key management is the fundamental challenge in achieving reliable secure communication using multicast key distribution for Mobile Ad hoc Networks. Multicast key distribution has to overcome the challenging element of "1 affects n" phenomenon.

**References :**

1. Brian P. Crow, Indra Widjaja, Jeon Geun Kim and Prescott T. Sakai, "IEEE 802.11 WirelessLocal Area Network," IEEE Communication Magazine, Vol. 35, No. 9, pp105-109,2015.
2. T. Kaya, G.Lin, G. Noubir, and A. Yilmaz, "Secure multicast groups on ad hoc networks" Proc. 1st ACM workshop on security of ad hoc and sensor networks, ACM Press, pp 94-102, 2017.
3. M. Ilyas, "The Handbook of Ad Hoc Wireless Networks," CRC Press, 2003.
4. Arun Kumar B. R., Lokanatha C. Reddy, Prakash.S.Hiremath , "Mobile Ad Hoc Networks: Issues, Research Trends and Experiments," International Engineering & Technology (IETECH) Journal of Communication Techniques, Vol. 2, No. 2, 057- 063, 2008.
5. M. Ilyas, "The Handbook of Ad Hoc Wireless Networks", CRC Press, 2003.
6. C. Perkins, "Ad hoc Networks," Addison-Wesley, 2001.
7. Chakrabarti and A. Mishra, "Quality of service challenges for wireless mobile ad hoc networks," Wiley J. Wireless Communication and Mobile Comput.vol. 4, pp.129-153, Mar 2004.
8. Scott Corson and Joseph Macker, "Mobile Ad Hoc Networking (MANET):Routing Protocol performance issues and evaluation consideration (Internet - Draft)", draft- ietf-manet-issues-01.txt, March 1998.
9. T. Kaya, G. Lin, G. Noubir, and A. Yilmaz., "Secure multicast groups on ad hoc networks",In Proceedings of the 1st ACM workshop on security of ad hoc and sensor networks, pp. 94 –102, 2003.
10. N.Kettaf, H Abouaissa and P. Lorenz, "An efficient heterogeneous key management approach for secure multicast communications in ad hoc networks, Telecommunication

❒❒❒