ISSN 2047-3338

Performance Analysis of Cluster Based Secure Multicast Key Management in MANET

Vineetha S. H[1]. and Shebin Kurian[2]

[1,2]School of Information Technology & Engineering, VIT University, Vellore, TamilNadu, India

[1]vineetha.s.h87@gmail.com, [2]shebinkurian@gmail.com

***Abstract*— Mobile Ad-hoc Network (MANET) is a group of wireless nodes join together to form a network without a defined architecture. It is formed dynamically as the nodes are mobile in nature. This characteristic of MANET could lead to insecure information exchange. Applications in Mobile Ad-hoc Networks (MANET) such as military or public emergency network require secure multicast communication. Multicasting supports group oriented communication. A cluster based system provides easy key management within a cluster or a group. In such an interaction system, a new member can join and a current member can leave at any time. This overcomes the issues of energy consumption, end to end delay, unreliability with high packet drop rate and low key delivery ratio. Also, the communication among the existing members can be made secure by using an efficient key management technique. The proposed method is efficient and more suitable for secure multicast communication dedicated to operate in MANETs. Performance analysis of non-clustered and clustered method of key management in MANET is done.**

***Index Terms*— Clustering, Hybrid Encryption, Multicasting and Secure Key Distribution**

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) does not have a centralized server. It is a type of wireless network which does not rely on an already existing infrastructure. A node for information exchange is made dynamically based on the network connectivity [1].Clustering is used to implement efficient communication in MANET [2]. Grouping nodes which have similar properties or divided large ad-Hoc network into smaller group is called clustering [6].This will overcome the difficulties of individual nodes by using efficient clustering technique. Clustering helps to achieve scalability and improve the performance of networks. Therefore it is suggested to maintain Cluster head (CH), cluster member, cluster gateway in cluster.

Multicast technique is employed to implement group oriented communication in MANET [10]. Security is a crucial task in multicast communication in MANET due to its dynamic nature. Authentication, data integrity, access control and group confidentiality are required in secure multicast communication. In communication keys are distributed to the group. These keys must be transferred securely among the existing users by using some sort of encryption decryption mechanism. Hence an efficient key distribution technique needs to be adopted which is a primary challenge on security.

In secure multicast system, group confidentiality, should be facilitated in order for communication system to be a reliable one. Several services need to be implemented to prevent attacks and eavesdropping so that to ensure authenticity, data integrity and data confidentiality in the group [1], [10]. Ensure security in multicast communication by using efficient key management scheme. The key management technique performs the creation, distribution and updation of the keys [1]. Efficient key management technique provide above services effectively. In this, hybrid encryption technique [8], [11] is used to encrypt and decrypt multicast data. Hybrid encryption technique is a combination of symmetric and asymmetric encryption technique.

A secret key is shared to a group in order to encrypt and decrypt messages and thus to ensure only group members (having the valid ID) would be able to access the data sent to a group. Hence, if a new member joins the group and if an existing member leaves the group, the key needs to be updated to maintain forward and backward secrecy [1], [10]. If the frequency of change in membership of the nodes in the group is quite often, then this rekeying technique could be a critical problem in key management. It may result in unreliability due to high packet loss rate and low key delivery ratio. This is called 1-affect-n phenomenon because change in a member would affect all the members in the network.

Multicast clustering is one of the suggested methods to overcome this problem. It is a method of dividing the nodes in the network to several groups such that each group is managed by a local controller (LC). Thus if a membership change occur in a cluster, the rekeying process will be local to that cluster alone. It does not affect other clusters in the network.

II. RELATED WORK

Key management approaches can be divided into three: i). Centralized, ii). Decentralized, iii). Distributed [1], [10].

In Centralized approaches, central server is responsible for generating and distributing key to all users in the network. In

distributed approaches, group members together can generate group key, this will helps to reduce bottleneck in network. In decentralized approaches, multicast network divided into different group or cluster. Each group or cluster consist cluster head (CH) and these CH head handle key distribution to group members. CH is responsible for secure key management.

CBT is cluster based multicast tree algorithm is used for secure multicast key distribution [1], [10]. Here each cluster have multicast connectivity between nodes. This algorithm is to elect local controllers for the created clusters. In CBT, CH can be easily elected by using information of nodes join and leave. In multicast tree, reduce retransmission by sending acknowledgement to cluster head. This algorithm overcomes fault tolerance occurs due to node failure and end to end delay.

In cluster based multicast, multicast group is divided into subgroups is called as clustering. Each cluster can accommodate up to some maximum number of nodes. When the maximum number is reached, the next new node will be connected to a new cluster (say cluster 0). If this node happens to be first node in that cluster, it will act as the Local controller for rest of the nodes in the same group. The advantage of applying clustering is that the overhead of re-encryption will be minimized to an extent. Clustering is overcome 1-affects-n problem to an extent.

For secure multicast communication, when a member joins or leaves a group forward and backward secrecy should be maintained [1], [10].

- Forward Secrecy: In a multicast group, when a member leaves, it should not have access to any future key.
- Backward Secrecy: In a multicast group, when a member joins, it should not have access to any of the previous key.

Multicast transmission is not affected when a child node leaves the group whereas when a local controller leaves, it sends notification to the GC and the group members under the leaving LCs are grouped under a cluster based on the reachability information by a multicast routing protocol.

Xie Hai-Tao is proposed an ID based and cluster based key management for MANET [2]. Here delay rekeying technique is used for MANET. When there are new nodes to join, cluster head finds out the type of node whether it is a new node or roaming node from another cluster. Cluster head checks the authenticity of nodes .If a node from another cluster joins, and then the current CH contacts previous CH of the node and verifies the authenticity of node. It provides better performance and reduces the probability of malicious nodes.

In distributed group key management approaches, there is no central authority for handling generation and distribution of network key [3]. Users themselves generate network key by using simple computation. In large mobile ad hoc networks, it is difficult to use one group key for whole network because of traffic and computation cost of regenerating key. Hierarchical approaches for key management in mobile Ad hoc networks paper propose any node in network can initiate process of key generation and smaller size cluster helps to create an energy efficient mobile Ad hoc network [3]. Communication cost of rekeying can be reduced in small clustered networks.

III. PROPOSED SYSTEM

The proposed system is Efficient Cluster Based Secure Multicast algorithm used for multicast key distribution in MANET. In this algorithm the sender node uses a Multicast version of the Routing Protocol which reduces retransmission by sending acknowledgements for each transmission. This routing protocol stores multiple disjoint paths to each destination in the network in addition to other required parameters for creating optimal paths to every destination. It maintains an up-to-date view of the network thus providing every node in the network to have an available route to every other node in the network. There are situations in which data is lost to unavailability of paths. Also, due to congestion or a link breakage, the messages may be buffered in queue storage at the source node. Once the queue is full, there will be loss of packets. Such problems can be solved with the help of available alternate path details.

In order to handle mobility of nodes, group oriented communication and secure key distribution; the network can be grouped to many groups or clusters. Thus forward secrecy and backward secrecy can be maintained when a node joins or leaves a group. Each cluster is managed by a cluster head and all the cluster heads are maintained by a group controller. Cluster members will be the one hop neighbours of cluster head. When a node joins a network, it is authenticated by the group controller. Cluster will have a specific limit on the number of cluster members each cluster head can handle. When the limit is reached, no new additions are made to that cluster. Each node contains the following information in its storage.

i. Node type: Denotes whether the node is a cluster head, cluster member, group controller or Cluster gateway.
ii. Node Id: Unique identifier to authenticate the node in the network.

Cluster Head: Holds the value of current cluster head.

When a node joins a cluster, it first checks if it was part of the network or a new node. If it is a new node, group controller should authenticate it. If it was in another cluster, the cluster head communicates with the node's previous cluster head to verify its authenticity.

Hybrid Encryption is used for improved security. It combines asymmetric encryption and symmetric encryption. Key generation is done through a partial key cryptography in which a portion of the key is generated by the cluster head and another portion is obtained by the node such that the key is not known to any trusted third party making it more secure. The cluster head sends the partial key to a node in receipt of its node id and thus authenticating the node. If the node did not receive the partial key from CH even after sending the node id, it sends an empty buffer to CH. When the CH receives an empty packet from a particular node id, it resends the partial key again. The generated key is used as a private key. A public key is generated from this private key and send to cluster head and all other nodes in the cluster. In addition to this, another secret key is shared among the cluster members for symmetric encryption. The data is first encrypted using public key of the receiver and then using the shared secret key, thus providing additional security for the data transferred.

IV. IMPLEMENTATION

A MANET is created using Qualnet network Simulator. The MAC layer protocol used is IEEE 802.11.This protocol provides authentication and de-authentication for the stations joining and leaving the network. It also provides re-association for the stations to receive packets when moving from one cluster to another. Mobility of the nodes is achieved using Random Waypoint in which nodes move randomly independent of other nodes. They can move freely without any restrictions. Multicasting is done by creating a Multicast Group and using a Multicast routing protocol. Multicast group is created using Multicast Group Editor in which a multicast address is specified for each group. The join and leave time of each node within a group is specified. MCBR (Multicast Constant Bit Rate) is the application traffic used to multicast data. Passive Clustering is used and clustering improves the efficiency. Security protocol used is IPSec and ISAKMP. IPSec security protocol at the network layer provides cryptographically based security for IP such as access control, integrity, authentication and confidentiality. The files created for implementation are *.config* file for designing the network, .nodes file contains the nodes and their IP addresses, .member file contains the multicast group members and *.ipsec* file is used to store the security parameters used.

TABLE I: SIMULATION ENVIORNMENT IN QUALNET NETWORK SIMULATOR 5.0

Parameter	Content
Field size	1500m X 1500m
Node number	25
Topology	Random
Mobility Model	Random Waypoint
Simulation Time	15 minutes
MAC Protocol	IEEE 802.11
Clustering Enabled	Yes
Security Protocol	IPSec, ISAKMP

The Fig. 1 illustrates the MANET created using Qualnet.

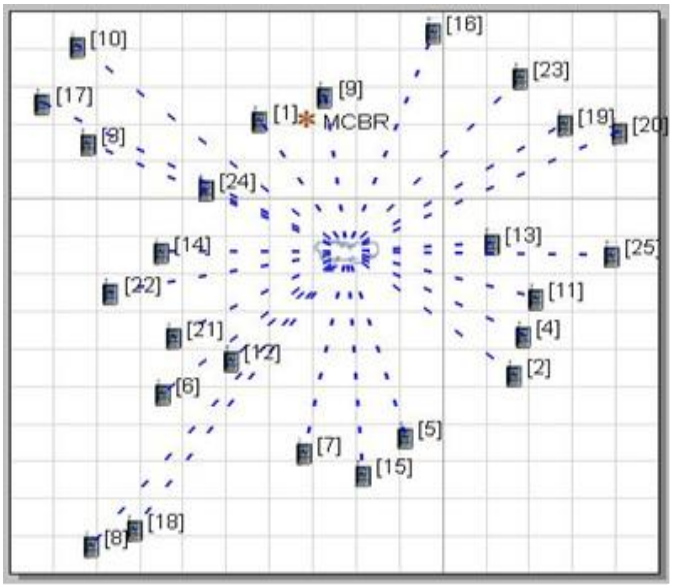

Fig. 1. MANET created in Qualnet

The Fig. 2 illustrates the packet transmission.

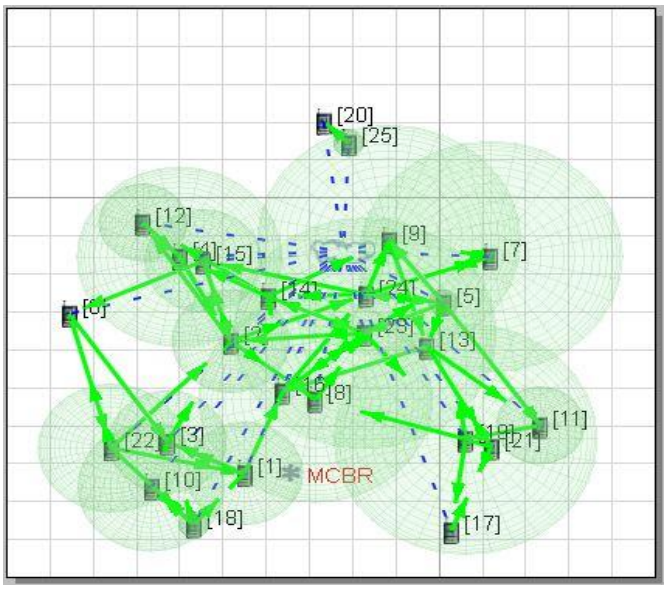

Fig. 2. Packet Transmission

The Fig. 3 illustrates throughput at different nodes for clustered and unclustered network.

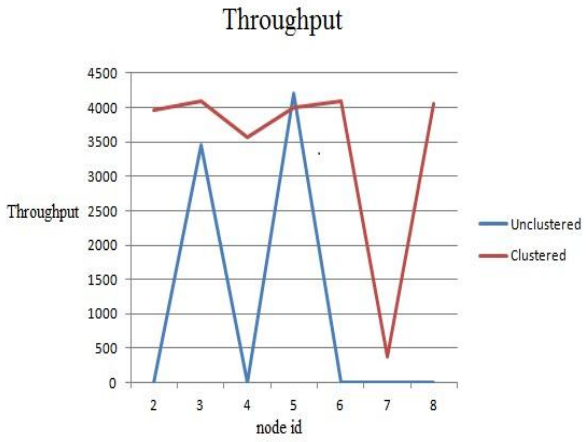

Fig. 3. Throughput at different nodes for clustered and unclustered network

The Fig. 4 illustrates Average End-to-End Delay at different nodes for clustered and unclustered network.

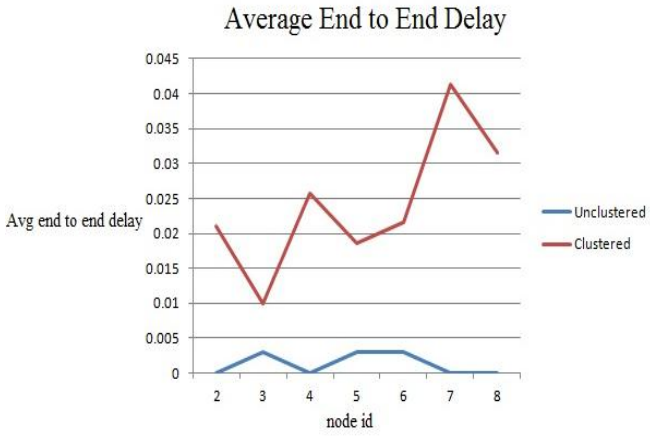

Fig. 4. Average End to End Delay at different nodes for clustered and unclustered network

The Fig. 5 illustrates total packets received at different nodes for clustered and unclustered network.

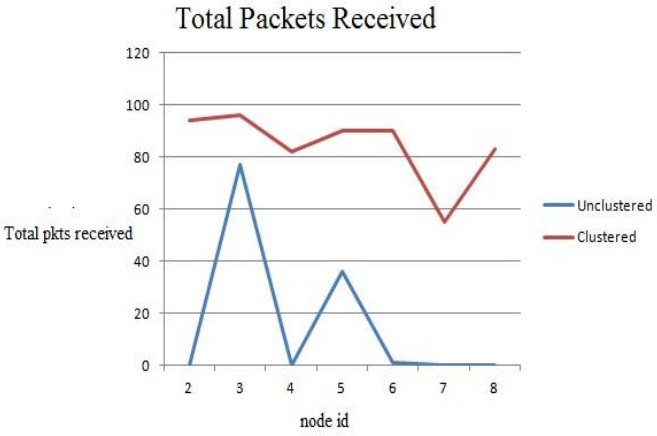

Fig. 5. Total Packets Received at different nodes for clustered and unclustered network

V. CONCLUSION

A comparison study is done on the performance metrics such as Average End to End Delay, Throughput and Packet Loss Rate in MANET key management with clustering and without clustering using Qualnet network simulator. It can be observed from the results that average end to end delay, total packets received and throughput are improved by clusterization.

REFERENCES

[1] K.Gomathi, B .parvathavarthini, "An Efficient Cluster based Key Management Scheme for MANET with Authentication", IEEE conference in Trendz in Information Sciences &Computing (TISC), Pages 202-205, 2010

[2] Xie Hai-tao, "A Cluster –Based Key Management Scheme for MANET ", IEEE conference in Intelligent Systems and Applications (ISA), Pages 1-4 ,2011

[3] Renuka A, K.C Shet, "Hierarchical Approach for Key Management in Mobile Ad hoc Networks ", IJCSNS International Journal of Computer Science and Network Security, VOL. 9 No. 4, April 2009.

[4] Yuan Zhang, Yongluo Shen, Sangkeun Lee, "A Cluster – Based Group Key Management Scheme for Wireless Sensor Networks", IEEE Web Conference (APWEB), 2010 12th International Asia-Pacific, Pages 386-388, 2010.

[5] Yao Nianmin, Ma Baoying, Fan Shuping, "A New Key Management Scheme in Clustering Wireless Sensor Networks" IEEE Conference in Internet Computing for Science and Engineering (ICICSE), 2009 Fourth International Conference on Computing & Processing (Hardware / Software), Pages 227-230, 2009.

[6] S. Jabeenbegum, Dr. T. Purusothaman, Karthi.M, Balachandar.N, ArunKumar. N, "A cluster based cost effective contributory key agreement protocol for secure group communication", IEEE Conference in Computing Communication and Networking Technologies (ICCCNT), 2010 International Conference on Communication, Networking & Broadcasting ;Computing & Processing (Hardware/Software), Pages 1-12 ,2010

[7] Wan An Xiong, Yao Huan Gong, "Secure and Highly Efficient Three Level Key Management Scheme for MANET ", ACM Journal WSEAS Transactions on Computers, Vol 10 Issue 1, Pages 6-15, January 2011

[8] Edna Elizabeth N, Vaidyanathan A, "Self-Healing Certificate less Hybrid Encryption", IEEE Conference in Communication Systems and Network Technologies (CSNT) 852-857, 2012.

[9] Sayegh, A.A.; El-Hadidi, M.T. "A Modified Secure Remote Password (SRP) Protocol for Key Intialization and Exchange in Bluetooth Systems" Security and Privacy for Emerging Areas in Communications in Networks, 2005. SecureComm 2005. First International Conference on Computing & Processing (Hardware/Software) , Pages 261-269, 2005.

[10] D. Suganya Devi, Dr. Padmavathi.G " Energy Efficient CBMT for Secure Multicast Key Distribution in Mobile Ad Hoc Networks", International Journal of Engineering Science and Technology Vol. 2(5), Pages 248-255, 2010.

[11] Renu Dalal,Yudhivr Singh, Manju Khari, " A Review on Key Management Schemes in MANET " International Journal of Distributed and Parallel Systems (IJDPS) Vol. 3, No. 4, July 2012.