SECURE MULTICAST KEY DISTRIBUTION IN MOBILE AD HOC NETWORKS

Prof. Sagar H. Thakare, Assistant Professor,
NCRD's Sterling Institute of Management Studies
sagarthakare@ncrdsims.edu.in

ABSTRACT
Since they enable users to obtain information and communicate from anywhere at any time, wireless networks and network devices are well-known. However, wireless communications are typically supported by a fixed infrastructure. To connect to a main station, a wireless device would use a single hop wireless transmission. Ad Hoc Network configuration, however, is less. In an ad hoc network, communication occurs between components in all directions.
The suggested work will be applied to create virtual clusters across networks. The other nodes in a cluster are known as member nodes, and each cluster has a cluster leader. In addition to these, the cluster head's member nodes have other characteristics. Key Management for secure cluster communication in Ad Hoc Networks is the primary concept of this project proposal.
Keywords: Advanced Cluster based multicast tree, Multicast Key Distribution in network, MANET.

Introduction

The need for computers in our everyday lives is driving up communication requirements,working on wireless solutions for Internet connectivity, email viewing and transmission, updating conference materials, and other uses. These criteria have outcomes. Ad hoc networks are in demand right now. Without a need for an external framework, they can be put up anywhere. Mobile Ad hoc Networks is another name for it. (MANET). Each component in the autonomous mobile ad hoc network (MANET) serves as both a router and an end system for all other groups in the network. When there is no access point accessible, the IEEE802.11 Wi-Fi protocol is used for Ad hoc network deployments at low positions.

Mobile Ad hoc Networks (MANET): Due to architecture, conservation, organization, and social surroundings, Mobile Ad hoc Network (MANET) plays a significant part in modern society. In a MANET, every group is mobile, and there is no set framework for the topology, which changes regularly. Tablets, mobile phones, computers, and other devices can all be shared in parties. Each device has the ability to transmit messages for other organizations as well as serve as a router.

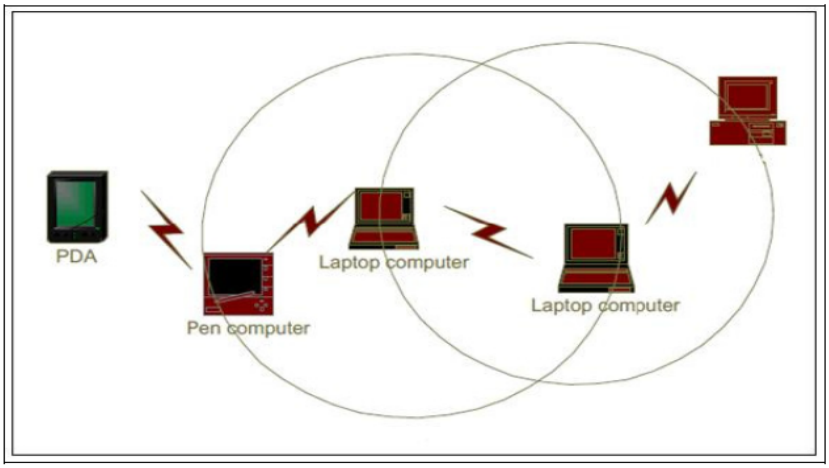

Figure 1: Structure of MANET (Source: Ilyas M. "The Handbook of Ad Hoc Wireless Networks", CRC Press, 2003)

Requirements of Key Management: Each node in a wireless multicast transmission is in possession of a key that can be used to encode and decode the multicast data. To comply with the multicast key management standards, the key must be updated and disseminated to all group nodes whenever a node enters or departs a group. For requirements, it is important to examine the key control procedure. These specifications are shown in Figure 2.

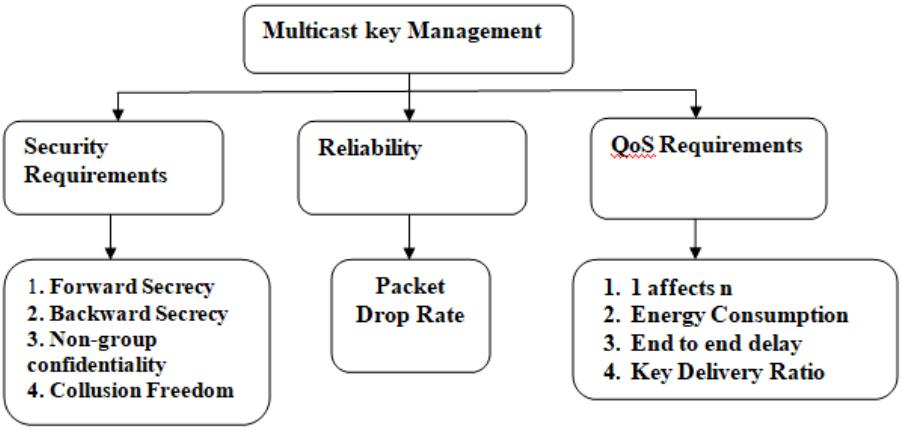

Figure 2: Role of Multicast Key Management

Literature Survey

Brian, Widjaja, Kim & Sakai (1997), according to above author they found the Wireless Computing is fleetly arising technology furnishing with network connectivity without being thread off a wired network. Wireless network want the same services and capabilities that they have generally come to anticipate with wired network. Physical and environmental necessity is another driving factor of WLAN.

Bettahar, Bouabdallah & Alkubeily (2007), according to author They focus on secure multicast communication's group secrecy, authentication, data security, and access control. Confidentiality plays the most crucial part in delivering several activities among that group.

Bouassida, Chrisment & Festor (2008), this strategy evenly splits the group and begins a multicast session with a concentrated method of operation. A dynamic clustering method for multicast means of dissemination in ad hoc networks is called Optimized Multicast Cluster Tree. This suggested quicker packet distribution and less energy usage. The primary goal of it is to establish new groups. The GPS coordinates of each group member are required for the creation of the Optimized Multicast Cluster Tree.

Chiang & Huang (2003), they discovered Mobile Ad Hoc Network through their study. It is a separate gathering of mobile groups that provides an unstructured setting for wireless conversation. Without any prior preparation, it emerges. Multicasting is group communication that includes sharing videos, participating in online conferences, participating in debate groups, getting stock alerts, and advertising. Multicast activities are made possible by the mix of ad hoc services.

Challal & Seba (2005), According to author they discovered that private multicast communication processes also use key transmission, updating, creation, and deletion. Each node selects a key to encode or decrypt the multicast data during a safe multicast connection. To maintain order and fulfill the multicast essential action, the key must be updated and distributed to all group members when a person enters and departs.

Liu (2007), According to this author they were working on distance vector routing algorithm, they discovered that each route in DSDV had a sequence number that began with the location and showed how ancient the route was. Here, there are two methods for conducting routing updates: "full group," in which a node communicates the entire routing table, and "incremental update," in which a node sends changes made since the previous update. The moment when a path becomes stable is determined using the distance vector routing algorithm.

Rahman & Zukarnain (2009), According to this author they perform the Destination Sequenced Distance Vector routing algorithm was developed for mobile ad hoc networks. As a fallback store, this protocol retains the routing database. As members of the group join and depart, data is exchanged in the routing table and routes are periodically kept. The increase of the distance vector influences the choice of route. It has a distinct sequence number that is updated on a regular basis and prevents misunderstanding nodes. It is also used for transportation within clusters. It permits quick reaction to structure changes.

Suganyadevi & Padmavathi (2010), According to author network achieves minimal packet loss rates and confidence. In order to save energy, the source group in this paper's safe multicast crucial dissemination system employs a multicast interpretation of the Destination Sequenced Distance Vector (MDSDV) routing algorithm. Additionally, it lessens multicast broadcast end-to-end latency.

Valle & Cardenas (2005), they discovered that encryption is a crucial instrument for attaining security. Security is provided to both sides of the network using cryptography. The primary component of an ad hoc network's security is critical function. In the ad hoc network, some symmetric and asymmetric key encryption operations are crucial. Key management processes include key generation, dissemination, storing, updating, as well as revocation, deletion, and arching.

Proposed Methodology

Advanced CBMT

The primary concept of the Advanced CBMT algorithm that I've suggested here is to use the Mobility aware Multicast DSDV routing protocol to elect the local controllers of the newly formed clusters while taking node failure into account. For safe transmission, the CBMT method creates a cluster-based multicast tree. Topology alterations brought on by node failure, however, may differ depending on how many individuals make up a cluster. This could lead to multiple transmission issues. Therefore, taking into account the size of each new cluster, an enhancement to the CBMT algorithm is crucial in order to tolerate the errors brought on by node failure. The following stages explain the proposed clustering approach's basic idea.

Advanced CBMT Algorithm

When the nodes are chosen as local controllers for the remaining group members because neither its clusters nor the newly formed clusters yet fully encompass all of the group members. The methods below are used when a node is mobile. When a node fails or is added to a cluster, the load on that cluster rises, making it difficult to elect a new LC.

Step-I

Due to membership dynamism, if a cluster has more group members than the maximum level, it must be divided up and a new LC chosen based on information about one hop distance reachability.

Step -II

Traverse the mass that has developed, Traverse the group members of this cluster and attempt to move them to the closest cluster if the cluster has fewer group members than the minimal criterion. As a result, the CBMT approach's effectiveness is increased while creating highly correlated groups based on the two criteria. As a result, this strategy is regarded as an Advanced CBMT. The advancements in the multicast key distribution algorithm using the advanced CBMT with mobility conscious MDSDV method are described.

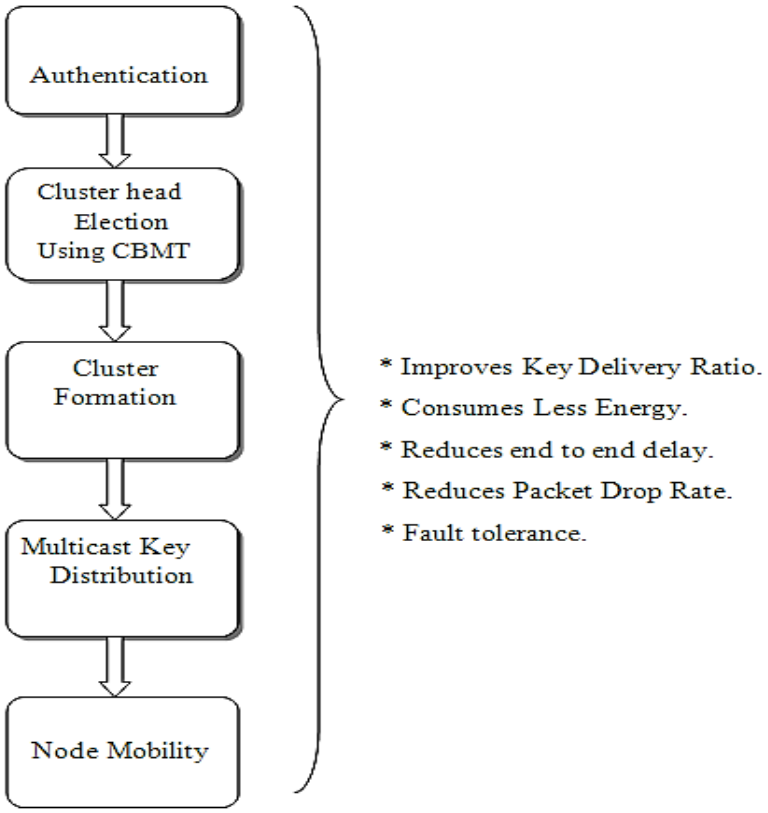

Figure 3: Proposed flowchart of advanced CBMT

Performance Metrics

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

- Packet drop ratio
- End to End delay
- Key delivery ratio
- Energy consumption
- Fault tolerance.

End to End Delay: It provides information about the typical latency or end-to-end delay of key transfer from the source to the recipients. This measure enables assessing the typical time it takes for an LC to forward a key to its cluster members.

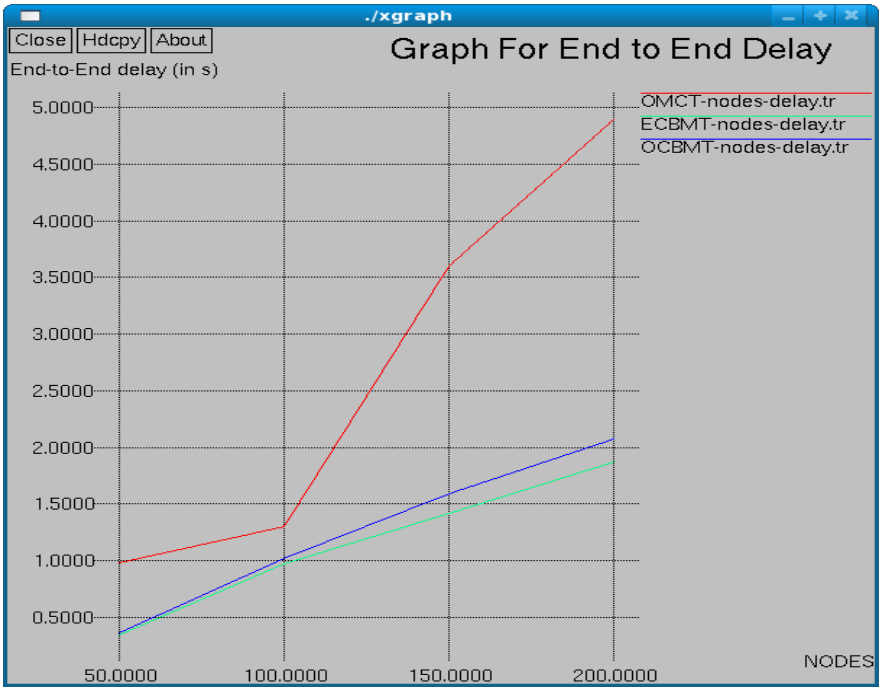

Figure 4: Graph for End to End Delay

Energy Consumption is the total amount of energy needed for key transfer over the course of multiplex data transmission.

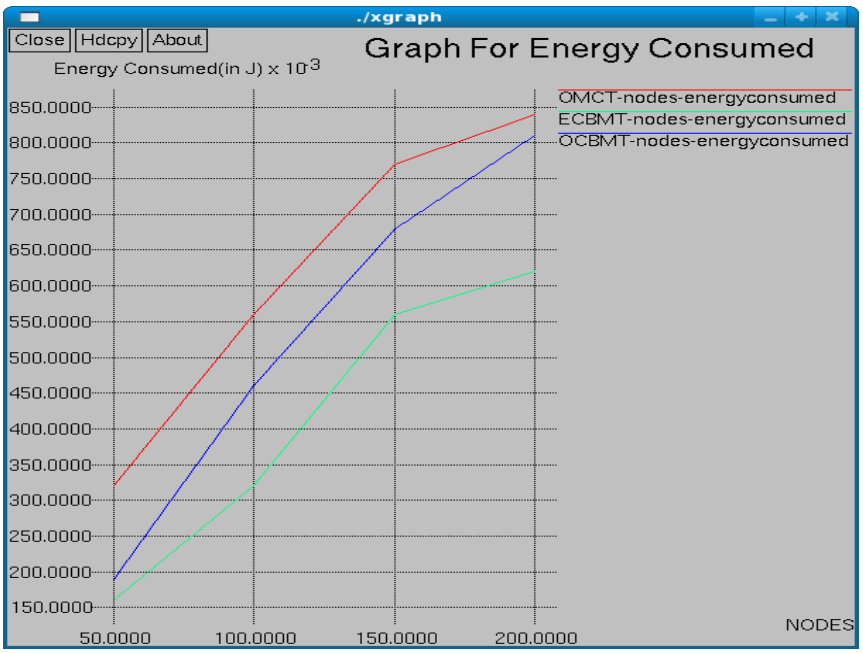

Figure 5: Graph for Energy consumption

Key Delivery Ratio The key delivery ratio is calculated by dividing the total number of sent and received keys. This measure enables assessing the protocol's dependability in terms of the success rate of key transfer from the source to group members.

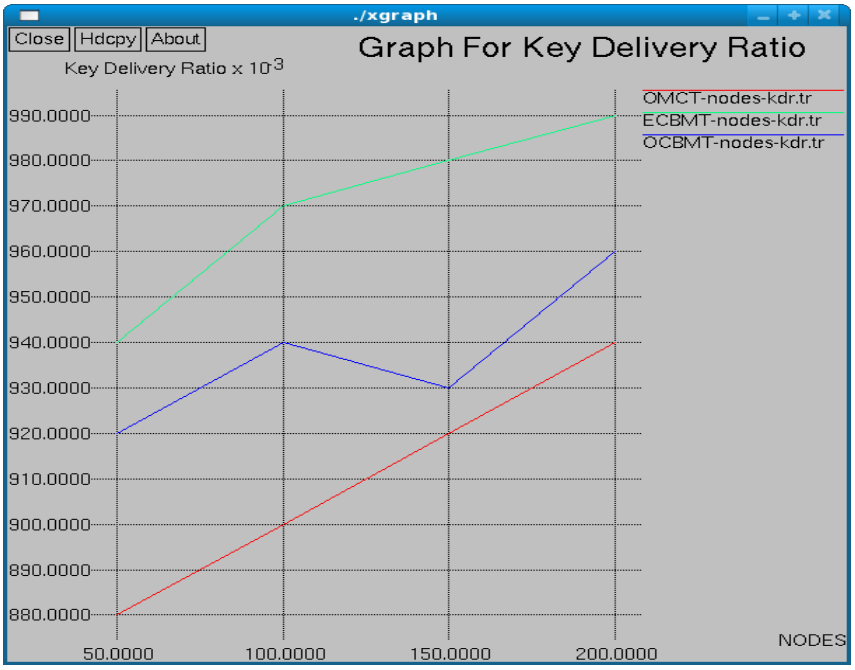

Figure 6: Graph for Key delivery ratio

Packet Drop Ratio: The percentage of packets sent to a location to those that are actually received there is known as the packet drop ratio. This measure percentage of packets lost during key transfer from the source to the group members.

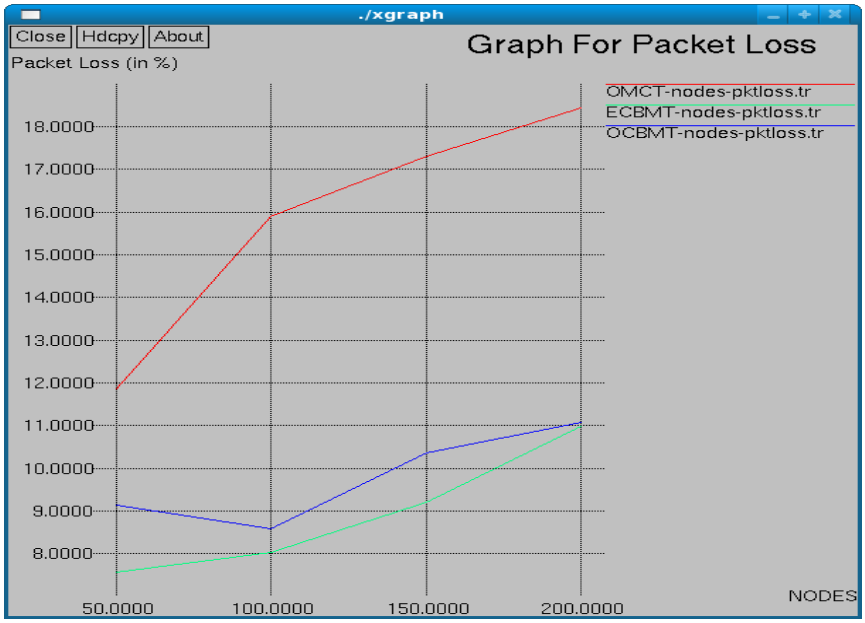

Figure 7: Graph for Packet drop ratio

Fault Tolerance: The fault-tolerance in key dissemination grows as the number of nodes rises. The multicast group is divided using this method while maintaining efficient communication between nodes. This is because it reduces the need for retransmission by sending feedback with each transfer. In contrast to OMCT, advanced CBMT tolerates the error that results from node failure of multicast transmission.

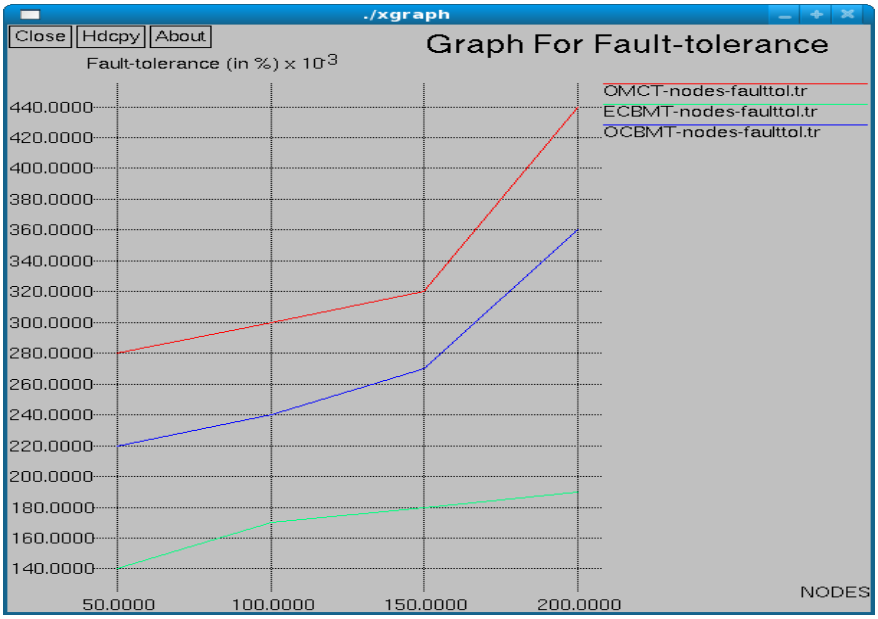

Figure 8: Graph for Fault tolerance

Conclusion

Group-oriented communication is a key component of many new apps for mobile ad hoc networks. Multicast is a useful tool for enabling group-oriented apps, especially in mobile environments with constrained power and bandwidth. Secure multicast communication is required for the use of such apps in a combative setting like the military. Due to the intrinsic QoS features of infrastructure-less architecture, secure multicast transmission in mobile ad hoc networks is difficult. High packet loss rates, an absence of a centralized authority, and scarce resources. Therefore, using multicast key distribution for Mobile Ad hoc Networks to achieve dependable secure communication presents the basic issue of key management. It is difficult to avoid the "1 affects n" phenomenon in multicast key dissemination.

References

Bettahar H., Bouabdallah A., & Alkubeily M.(2007), "Efficient Key Management Scheme for Secure Application level", In IEEE system on Computers and Communications, pp 489-497, (2007).

Brian C., Widjaja I., Kim J.& Sakai P.(1997), "IEEE 802.11 Wireless Local Area Network," IEEE Communication Magazine, Vol. 35, No. 9, pp 116-126, September 1997.

Bouassida M., Chrisment I. & Festor O.(2008), "Group Key Management in Manets", International Journal of Network Security, 67–79 (January 2008).

Challal Y., Seba H. (2005), "Group Key Management Protocols: A novel Taxonomy", In Proc. International Journal of Information Technology pp 105-118, (2005).

Chiang T., Huang Y. (2003),"Group keys and the multicast security in ad hoc networks", Proc. IEEE International Conference on Parallel Processing, IEEE press, pp 385- 390, Oct 2003.

Ilyas M. (2003), "The Handbook of Ad Hoc Wireless Networks", CRC Press, 2003.

Ilyas M. (2008), **"**The Handbook of Ad Hoc Wireless Networks," CRC Press, 2008.

Kumar A., Lokanatha C., Prakash.S. (2008), "Mobile Ad Hoc Networks: Issues, Research Trends and Experiments," International Engineering & Technology (IETECH) Journal of Communication Techniques, Vol. 2, No. 2, 057-063, 2008.

Liu T., Liu K. (2007)," Improvement on DSDV in Mobile Ad Hoc Networks", In IEEE, China, pp.1637-1640, (2007).

Perkins C.(2001), "Ad hoc Networks," Addison-Wesley, 2001.

Rahman A., Zukarnain A. (2009), "Performance Comparison of AODV, DSDV and I-DSDV routing protocols in Mobile Adhoc Networks", In: European Journal of scientific Research, pp 566-576, (2009).

Suganyadevia D., Padmavathib G. (2010), "Energy Efficient CBMT for Secure Multicast Key Distribution in Mobile Ad Hoc Networks", Procedia Computer Science 2 ,pp 248–255, (2010)

Valle G., Cardenas R.(2005), "Overview the Key Management in Adhoc Networks", In LCNS 3563, pp 397-406, (2005).

