An Exclusive Survey on Cluster Based Key Management Techniques in MANET

[1] K. Gomathi, [2]Dr. B. Parvathavarthini
[1] Research Scholar, [2] Professor & Head,
Sathyabama University,Chennai

***Abstract*--- Without employing tough security features, group communication in MANET cannot provide privacy to its group members. In this aspect encryption key(Group key) has to be established between the members for safe and sound group communication. The group key management in MANET is very critical, since frequent node movement, link failures, resource drainage and without centralized control. To cope with these characteristics variety of clustering concepts emerged, to aggregate MANET nodes into subgroups that accomplish network management easier. The combined effect of clustering and key management achieves greater heights in security among group members. This paper presents generous survey on various cluster based group key management in MANET and also discussed about specific features and limitations of every protocol.**

***Index Terms*— Clustering, Group Key Management, MANET**

I. INTRODUCTION

The primary method used for transferring data among group member is multicasting and secure groups are constructed using encryption schemes. The data flow in group communication are protected by encryption using some cryptographic keys also known as Group Key. As a result outside members cannot decode data without knowing Group key. The Group key management in MANET face greater challenges due to without fixed infrastructure, varying scalability, node mobility, limited resources, limited bandwidth and no centralized control.

II. RELATED WORK

The Group Key management techniques that include generation, distribution and updating of the key whenever changes in membership of the group. In general there are three different approaches used for generating Group keys[1].

a. Types of Group Key Management Techniques

- Centralized Group Key Distribution (CGKD)-- Single entity or key server responsible for creation, distribution and modification whole group key management however this may cause overload on single entity.
- De-Centralized Group Key Management(DGKM)-- Multiple entities responsible for group key management. Large network divided in to small sub group and subgroup controller taken the responsibility of key management. The nodes grouped under hierarchical manner, implementation is difficult.
- Contributory/ distributed Group Key Agreement(CGKA)-- Members themselves responsible for Group Key management. For Secure Group Communication(SGC) mostly prefer this type of key agreement, since Trusted Third party(TTP) not available for group key management and moreover all work equally shared by associated members no burden for single entity. But main limitation is not scalable.

The membership changes require frequent change of GK and this ensure the Forward and backward security. The GK can be changed either periodically at particular interval of time(batch rekeying or delayed rekeying) or for every membership change. some of the basic requirements considered before adopting any key management.

- Ensure Forward Security: already left members may not know the future communication.
- Ensure Backward security: newly joined members cannot determine the past communication.
- Key independence and resilience
- support for scalability and service availability
- Less computation, communication and storage cost

In this centralized approach is unsuitable for wireless network like MANET due to the following reasons like lack of scalability, inability to support membership change and 1-affects- n problem. In this single server manages group key for entire communication its inadequate for dynamic network like MANET, however more suitable for fixed, wired and less dynamic network.

b. Need for Clustering

Rekeying or refreshing GK for large and dynamic group is difficult one, because MANET devices are energy constrained, bandwidth constrained, battery operated and wireless devices. One of the proposed architecture for efficient resource and Group key management in MANET, is **clustering.** The clusters are sub groups of large network that simplifies group key management by rekeying done only for affected clusters not for entire network while mobile node movement.

Also clustering simplifies routing overhead, while inter cluster communication paths stored only about clusters not about individual nodes and for intra cluster communication nodes having information about its cluster members not entire network. Every cluster consists of one cluster head (CH), one gateway and many member nodes. The CH node act as a local controller for managing keys inside the cluster.

c. Types of Clustering Approaches

The clustering categorized into different approaches based on the metrics considered for clustering.[2] They are

- Node ID-based clustering

The unique identifier is assigned to all the nodes. The Node with the minimum ID is selected as cluster head by broadcasting Hello message to its neighbor.

- Connectivity based clustering

The node with the maximum number of neighbors within its transmission range is selected as cluster Head.

- Mobility- metric based clustering

The mobility metric taken consideration for cluster formation process. Moreover, clusters is formed in such a way that mobile nodes with relative speed to their neighbors and mobile node with low speed have the chance to become cluster heads.

- Energy or Battery power based clustering

Energy consumption pose a meticulous challenge for MANET. The Cluster Head is selected based on the energy level of the node.

- Combined weight based clustering

Weight based clustering techniques use several metrics such as: mobility, connectivity, battery Power and transmission range. Based on these combined metrics CH is selected.

III. SURVEY OF CLUSTER BASED GROUP KEY MANAGEMENT PROTOCOL

This survey clearly summarize the uniqueness and disadvantages of the each and every protocol.

Survey on Cluster based Group key Management Protocols

CH selection/ type of clustering	Structure/ arrangement of Nodes	uniqueness of the protocol	Limitations	Group Key Management Type	Reference No
Smallest id among all neighbors	Balanced hash tree	• CH generates GK using AES(Advanced Encryption Standard. • By using hash value and public key GK is distributed	Without caring any other metric the node with smallest id is considered as CH.	Decentralized cluster based approach	[3]
Based on Location identification number	Tree based GK Management	• Source authentication by RSA and DH used for common key generation. • Location identification number(LID) and Cluster Identification Number(CID) provided by offline authority.	Offline authority needed for communication.	Distributed Group key agreement	[4]
Based on lowest id	Flat structure	• Hash function is used for authentication, monitoring node used for network connectivity. • CH generates GK by receiving public keys of member nodes	Id only considered for CH election, this may lead to incompatible node as CH	Distributed or contributor key management	[5]
CH election based on combined weight metrics(Battery power, Mobility, Degree Difference, Distance)	Flat network topology	• Secondary CH elected to cope with CH in case of sudden death of CH • Nodes Public Key used to create GK	Computation overhead is high. Even though weight based clustering considers all factors, but not considering trust factor.	Contributory key management	[6]
Better connectivity node	Hierarchical structure	• Nodes gain a key pair from Key Generation Center(KGC) before joining the	Due to delayed rekeying policy	Decentralized approach.	[7]

		network. • Every member receives nonce from CH and signs this nonce by private key	fraudulent node may interfere in the communication.	Cluster key generated by CH using polynomial function. Delay rekeying policy.	
Trust Based clustering. The node with highest Total Trust(TT) elected as Cluster Head.	Tree based GK Management	• Evict malicious node from communication • Excessive communication overhead is reduced.	Periodic Hello message send to neighbors to get network information. This may increase traffic inside the network.	Contributory key management	[8]
Clustering done based on nodes which have fair key and uses minimum number of resources and bandwidth	Tree based multicasting	• The activities of the nodes are monitored and the keys are assigned • FRKS-Fair key and resource scheduler for cluster based multicasting	Minimum resource consumption node elected as CH, but not less mobile node.	Centralized key management	[9]
Trust based clustering	Tree based structure	• Malicious node being avoided by exchanging trust value. • CH and auxiliary node termed as control set. • control set members contribute to form a TEK	Direct and Indirect trust are calculated for identifying CH. This leads to excessive calculation.	Contributory key management(A.GDH2 is used for key contribution)	[10]
Regional leader elected with smallest id.	MDS code based key tree.	• Assumed each member of system is equipped with GPS • Partitions group into region based subgroups based Novel Rekeying function protocol. • MDS (Maximum Distance Separable)code(error control code)is used for multicast key distributions	Only suitable for node with GPS	Decentralized key management. (Region based Group key management)	[11]

IV. CONCLUSION

The objective of this study is to encourage more researchers to find most optimal solutions in Cluster based Group key management according to the application area. All the three types of Group key management have their own merits and demerits however Contributory Key management is most suitable one for Secure Group communication. The survival of fraudulent nodes in the network provoke various complication in network. Sometimes this may guide to entire failure of communication due to consumption of valuable resources. In our perspective Trust based clustering considered best among other clustering schemes since it isolates misbehaving node from the network. So no one Cluster based Group Key Management(CGKM) satisfy all the requirements, based on the application scenario, suitable CGKM can be applied.

REFERENCES

[1] Trust Tshepo Mapoka, " Group Key Management protocols for Secure Mobile Multicast Communication: A Comprehensive Survey", International Journal of Computer Applications, Vol 84, No. 12, December 2013, pp 23-38.

[2] Abdelhak Bentaleb, Abdelhak Boubetra and Saad Harous, " Survey of Clustering Schemes in Mobile Ad hoc Networks", scientific Research, Communications and Network, Vol 5, May 2013, pp 8-14.

[3] Renuka A. and K.C. Shet " Cluster based Group Key management in Mobile Ad hoc networks" International Journal of Computer Science and Network Security, Vol 9 No. 4, April 2009, pp: 42-49.

[4] Rajender Dharavath and K.Bhima, "Distributed Group key Management with cluster based communication for dynamic peer groups", Vol 2, N. 2, Febrauary 2011, pp 82-89.

[5] N.Suganthi and V.Sumathy, " An Efficient Key management scheme for Mobile Ad hoc Networks with Authentication", International Journal of Computer and Network Security, Vol 2 No. 5, May 2010, pp 103-107.

[6] K.Gomathi, Dr. B. Parvathavarthini, " An Enhanced Distributed Weighted Clustering Routing Protocol For Key Management", Indian Journal of Science and Technology, vol 8, Issue 4, Feb 2015, pp:342-348 (Scopus Indexed)

[7] Xie Hai-tao, " A Cluster based Key management Scheme for MANET" International workshop on Intelligent Systems and Applications", May 2011, pp 1-4.

[8] K.Drira, H.Seba, H.Kheddouci, :ECGK: An efficient Clustering scheme for group key management in Manets", Elsevier Computer Communications, vol 33,2010, pp 1094-1107.

[9] D.Anitha, M.Punithavalli, "Efficient Cluster based Multicast using Fair Key and Resource Scheduler for Social Network Communication in Manet", International Journal of Computer Technology and Applications, Vol 3 ,Issue 3, pp 1265-1272.

[10] V.Bhuvaneswari, M.Chandrasekaran, " Cluster head based Group key Management for Malicious Wireless Networks using Trust Metrics", Journal of Theoretical and Applied Information Technology, Vol 68, No. 1, October 2014, pp 1-9.

[11] N.Vimala, B.Jayaram, R. Balasubramanian, " An efficient Rekeying function protocol with Multicast key Distribution for Group key management in MANETs", International Journal of Computer Applications, Vol 19, No. 2, April 2011, pp 44-51.