An Exclusive Survey on Cluster Based Key Management Techniques in MANET

K. Gomathi, 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.

<table>
<thead>
<tr>
<th>Survey on Cluster based Group key Management Protocols</th>
<th>CH selection/ type of clustering</th>
<th>Structure/ arrangement of Nodes</th>
<th>uniqueness of the protocol</th>
<th>Limitations</th>
<th>Group Key Management Type</th>
<th>Reference No</th>
</tr>
</thead>
</table>
| 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]           |
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
