IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

A Survey Paper of Cluster based Key Management Techniques for Secured Data Transmission in Manet

K.E Hemapriya[1], K. Gomathy[2]

MCA, Research Scholar, Bharathiar University, Coimbatore[1]

MCA, M.Phil, Assistant Professor, Dept of Computer Applications, Dr.N.G.P Arts and Science College, Coimbatore[2]

Abstract: In Mobile Ad Hoc Networks (MANETS), Clustering based routing protocol can sufficiently enhance Performance, Scalability and Energy Efficiency. In this research Improved weight based clustering techniques integrated along with a routing protocol is proposed. Our approach is inspired from bird flocking behavior where birds travel long distances in flocks and conserve energy by constantly changing the leader of the flock. We have mainly concentrated on clustering algorithm and designed our clustering algorithm based on moment-to moment decisions of individual nodes during communication. In this protocol, the network is divided into chunks of nodes known as clusters. The clusters are actively maintained and reassembled using specific algorithms and techniques. Due to nature of inconstant wireless medium data transfer is a major problem in ad hoc it lacks security and reliability of data. Cryptographic techniques are often used for secure data transmission wireless networks. Most cryptographic technique can be symmetric and asymmetric, depending on the way they use keys. However, all cryptographic techniques is good for nothing if key management is weak. There is various type of key management schemes that have been proposed for ad hoc. Peer-to-peer computing is a popular paradigm for different applications that allow direct message passing among peers. The existing P2P search algorithms in MANET (Mobile Ad-hoc Network) are flooding-based search that produces much traffic and network overhead. File searching efficiency of peer-to-peer (P2P) network mainly depends on the reduction of message overhead. The research work deals with a full form of cluster based P2P file searching approach for MANETs, which focuses mainly over reduction of control messages. For searching, our mechanism uses cluster head within the cluster but it also allows inter-cluster communication. Moreover, secondary cluster head concept of our proposal ensures lower message overhead during cluster formation stage. Our clustering scheme utilizes request suppression to reduce the number of responses for searching process. Consideration of alternative paths to a node facilitates to overcome link failure. The improved weight based routing scheme is a position based routing approach which incorporates dynamic selection of the gateway nodes to reduce the number of control packets flooded in the network. The improved weight based clustering key management techniques increase the packet delivery ratio, reduce overhead and also reduces energy consumption in the network. The simulation study of proposed improved weight based clustering algorithm achieved better performance than the existing key management schemes. In this research overhead is reduced by 17%, energy consumption is reduced by 5% and packet delivery ratio is dramatically increased by 10%. Overall study of this research work achieves better performance compared with existing methods. This research work compares the efficiency of the proposed scheme with the existing schemes and the comparison shows that the proposed scheme performs better than the existing schemes in terms of reduction in key update messages.

Keywords: MANETS, Clustering Techniques, Routing protocol and Key Management

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) have received drastically increasing interest, partly owing to the potential applicability of MANETs to myriad applications. The deployment of such networks, however, poses several challenging issues, due to the dynamic nature of the nodes, the arbitrary topology, the limited wireless range of nodes, and transmission errors. Since all the nodes in the network collaborate to forward the data, the wireless channel is prone to active and passive attacks by malicious nodes, such as Denial of Service (DoS), eavesdropping, spoofing, etc. Implementing security is therefore of prime importance in such networks.

A MANET is system of wireless nodes that communicate over wireless links which are having limited bandwidth. Each wireless node can work as a sender, receiver, and router. When a node acts as a sender, it can send message to any destination node with some route. When it acts as a receiver, node can receive messages from any other node in the network. When the node will work as a router, it can send the packet to destination or the next router in the route. MANET has many advantages over traditional wireless networks such as speed of deployment, easy deployment, less dependence on fixed infrastructure. Therefore, there is an emerging wireless networking field

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

for future mobile communications. In moving towards MANET technology, the task of finding good solutions for the challenges such as security, routing, quality of service will play a crucial role for the success of Mobile Ad-hoc Network Technology. Security is an important and essential component for network functions such as packet forwarding and routing. The five components of a security mechanism are confidentiality, integrity, authenticity, availability and non-reputability. Out of these, authenticity is the most fundamental issue, since a breach of authenticity leads to a system-wide compromise. One of the widely used authentication mechanisms in conventional wired networks is the public key management system using certificates. One of the main issues to consider in a certificate-based scheme is the secure distribution of the public keys to all the nodes in the network.

The Public Key Infrastructure (PKI) [1] defines methods to handle public key management using X.509 certificates. In a wired network, there exists a centralized certificate server which handles the creation, renewal and revocation of certificates. This is not feasible in ad hoc networks, due to the absence of a fixed infrastructure and centralized management. Besides, due to the dynamic topology of the network, frequent link failures may occur, resulting in issues such as re-authentication and timely communication with the certificate server.
Recently, routing in MANETs has become one of the most challenging tasks. Routing in networking is the process of selecting paths in a network to send network traffic. A number of routing protocols techniques have been proposed for use in MANETs such as Ad-hoc on demand. Distance Vector Routing (AODV) , Dynamic Source Routing (DSR), and Destination Sequence Distance Vector (DSDV).

Clustering is an approach used to reduce traffic during the routing process. Clustering is division of the network into different virtual groups based on rules in order to discriminate the nodes allocated to different sub-networks. The goal of clustering is to achieve scalability in presence of large networks and high mobility. Roles of nodes in clusters are grouped in four categories namely cluster head, gateway nodes, member nodes and guest nodes. Fig. 1 shows categories of nodes in cluster.

1. **Cluster-head**: A Cluster-head node is the local coordinator of a cluster. The transmission range of cluster head describes the limitations of a cluster.
2. **Gateway Nodes**: Gateway nodes are located at the boundary of the cluster. It can forward information between clusters.
3. **Member Nodes**: Member nodes are also called as ordinary node. Member nodes are members of a cluster and these nodes have neighbours belonging to their own cluster.
4. **Guest Node**: Guest node is a node associated to a cluster.

In addition, it is common for ad-hoc networks to rely on multicast for management-related control traffic such as neighbor/route discovery to setup multi-hop paths, the establishment of time synchronization, etc. Such multicast traffic among the nodes has to be delivered in a secure and trusted manner. In particular the provided network services need to achieve the following security goals: Confidentiality, Message integrity and Source Authentication[2]. Confidentiality is achieved by encrypting the transmitted data. Providing an efficient multicast message and source authentication security service that can easily scale for large networks is an important capability for the operation and management of the underlying network. Source and message authentication is the corroboration that a message has not been changed and the sender of a message is as claimed to be. This can be done by sending a
(1) Cryptographic digital signature, or

(2) Message Authentication Code (MAC).

1.1 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[3].

1.2 Limitations of the Existing Key Management Protocols

The following are the limitations imposed by the existing symmetric and asymmetric key management protocols in MANETs:

- Symmetric key distribution requires a Centralized Authority (CA) authentication and key management among nodes.
- Secret keys have to be stored in key pool
- Frequent key refreshmen1 is needed by the CA
- Authentication process is time consuming and increase communication overhead.
- For larger networks the average number of hops to the CA increases which means the energy consumed for key requests and replies increases.
- Asymmetric key distribution like RSA requires larger Key silts
- Increased computational cost
- Increased power consumption and end-to-end delay.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

1.3 Objectives

The proposed research work achieves the following objectives:

- Clustering ensure sufficient data transmission.
- Clustering in MANETs using the prediction based hierarchical clustering network model.
- Cluster based routing model for secure transmission in MANET.
- Mutual Authentication and Session Key Management using ECC.
- Improved Weight based clustering algorithm achieves secure data transmission.

2. LITERATURE SURVEY

Key management is a very important part of any safe communication. Most cryptosystems rely on some necessary secure, robust, and efficient key management system. This section discusses some of the related proposed key management schemes for secure group communication in wireless ad hoc networks.

Most existing security mechanisms for MANETs thus far involve the heavy use of public-key certificates. Yanchao Zhang et al. in [5] presented an ID-based key management scheme as a novel combination of ID-based and threshold cryptography. IKM is a certificate less solution in that public keys of mobile nodes are directly derivable from their known IDs plus some common information. It thus eliminates the need for certificate based authenticated public-key distribution indispensable in conventional public-key management schemes.

Maghmoumi et al. in [6] proposed a cluster based scalable key management protocol for ad hoc networks. Their proposed protocol is related to a new clustering technique. The network is segregated into communities or clusters based on similarity relationships between nodes. In order to make sure the trusted communications between nodes they proposed two types of keys generated by each cluster head.

The protocol is adaptive according to the restriction of the mobile nodes battery power and to the dynamic network topology changes. This proposed approach of clustering is based scalable key management protocol provided protected communications between the nodes of the ad hoc networks.

A key management proposal for secure group communication in MANETs was described by Wang et al. in [7]. They illustrate a hierarchical key management scheme (HKMS) for secure group communications in MANETs. For the sake of security, they encrypted a packet twice. They also converse about group maintenance in their paper in order to deal with changes in the topology of a MANET. At last, they carried out a performance analysis to compare their proposed scheme with other conventional methods that are used for key management in MANETs. The results demonstrate that their proposed method performed well in providing secure group communication in MANETs.

Jin-Hee Cho et al. in [8] proposed a fully distributed trust-based public key management approach for MANETs using a soft security mechanism based on the concept of trust. They proposed a composite trust-based public key management (CTPKM) with no centralized trust entity with the goal of maximizing performance (e.g., service availability or efficiency) while justifying security vulnerability. Each node employs a trust threshold to determine whether or not to trust another node. Each node‟s decision making using the given trust threshold affects performance and security of CTPKM.

A new group key management protocol for wireless communication ad hoc networks was stated by Rony et al. in [9]. They put forth a well-organized group key distribution (most commonly known as group key agreement) protocol which is based on multi-party Diffie Hellman group key exchange and which is also password authenticated. The basic idea of the protocol is to securely construct and distribute a secret session key, among a group of nodes/users who want to communicate among themselves in a secure manner. The projected protocol starts by constructing a spanning tree on-the fly concerning all the valid nodes in the scenario. It is understood, like all other protocols that each node is individually addressed and knows all its neighbors.

Unlike several other protocols, the proposed approach does not need broadcast/multicast capability. Bechler et al. in [10] proposed cluster-based security architecture for Ad hoc networks. They proposed security concept based on a distributed certification facility. A network is divided into clusters with one unique head node for each cluster. These cluster head nodes carry out organizational functions and shares a network key among other members of the cluster. Moreover the same key is used for certification. In each cluster, exactly one distinguished node–the cluster head (CH)–is responsible for establishing and organizing the cluster.

Clustering is also used in some of the routing protocols for ad hoc networks. Decentralization is attained using threshold cryptography and a network secret that is distributed over a number of nodes. A scalable key management and clustering scheme was anticipated by Jason et al. in [12]. They estimated a scalable key management and clustering scheme for secure group communications in ad hoc networks.

The scalability problem is solved by segregating the communicating devices into subgroups, with a leader in each subgroup, and further organizing the subgroups into hierarchies. Each level of the hierarchy is called a tier or layer. The hierarchical flow is in order of Key generation, distribution, and actual data transmissions. Distributed

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

Efficient Clustering Approach (DECA) present a robust clustering to form subgroups, and analytical and simulation results demonstrate that DECA is energy-efficient and resilient against node mobility. Match up to other schemes, their approach is extremely scalable and efficient, provides more security guarantees, and is selective, adaptive and robust.

Clustering divides the network nodes into different virtual groups which are geographically adjacent and helps to organize the ad hoc networks hierarchically. A great number of heuristic clustering algorithms have been presented in the literature and in [13] Yu et al., discuss about the latest developments in clustering and categorize the existing clustering schemes as dominating-set based clustering, low-maintenance clustering, mobility-aware clustering, energy-efficient clustering, load-balancing clustering and combined-metrics-based clustering. Wei et al., classify the clustering schemes as single hop VS multi-hop schemes and location-based VS non-location-based schemes and stationary VS mobile schemes and asynchronous VS synchronous schemes. In addition, they analyze each category and illustrate their advantages and limitations [14].

Hegland, A.M. et al, in "A survey of key management in ad hoc networks" 2006 [15],describe the wireless and dynamic nature of mobile ad hoc networks (MANETs) leaves them more vulnerable to security attacks than their wired counterparts. The nodes act both as routers and as communication end points. This makes the network layer more prone to security attacks.

A main challenge is to judge whether or not a routing message originates from a trustworthy node. The solution thus far is cryptographically signed messages. This article surveys the classification of key management schemes based on contributory and distributive scheme. The analysis puts some emphasis on their applicability in scenarios such as emergency and rescue operations

3. CLUSTERING TECHNIQUES

3.1 CLUSTER FORMATION AND CLUSTER-HEAD SELECTION

The cluster formation phase is invoked when initializing node X does not receive any reply message. Cluster is formed primarily for the following two circumstances: Though there remain some member nodes of a cluster but unfortunately CH of that cluster is out of the range for initializing node X. The node X has no neighboring node(s) within its transmission range.

For these cases, cluster is formed with node X declaring itself as a Cluster Head as Fig. This newly formed cluster does not contain any cluster member because CH has no neighboring nodes for second case and for first case, though there remain some neighboring nodes of X, they are already a member of another cluster.

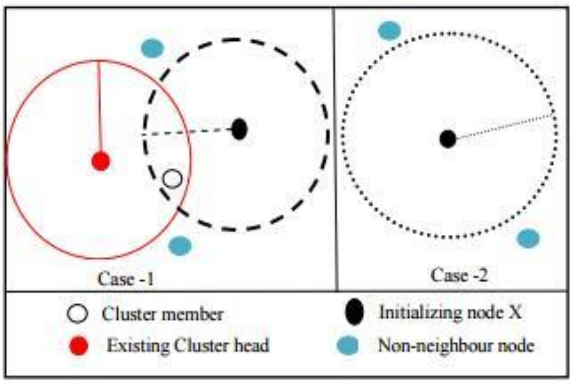

Figure 3.1. Initializing node X receives no reply message

Cluster Maintenance - Cluster-Head sends ALIVE message with its node ID and energy level to the member nodes of the cluster periodically. Let us consider this periodic time is T sec. Before sending the ALIVE message CH starts a timer TA. All the neighbouring nodes of cluster head receive the message and send acknowledgement to the CH. As the timer expired, CH checks its MEMBER_INFO table in order to find the members who have not send acknowledgement message but their entries reside in the table. The information of those nodes is deleted from the MEMBER_INFO table as the nodes are no longer a neighbouring node of the previous CH. On the other hand, all the member nodes except Secondary CH wait for T period. If it does not receive any ALIVE message from its CH, it again waits for T period to get ALIVE message from Secondary CH. When a member node receives ALIVE message from Secondary CH, it joins under that CH by sending JOIN message. Otherwise the node checks whether it has received ALIVE message from other CHs within this 2T period.

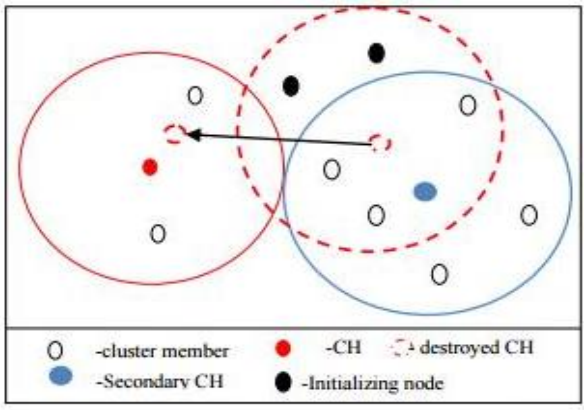

Figure 3.2 Cluster Maintenance

3.2 CLUSTER BASED ROUTING IN MANETS

The process that divides the network into interconnected substructures, called clusters. Each cluster has a particular node elected as cluster head (CH) based on a specific metric or a combination of metrics such as identity, degree, mobility, weight, density, etc.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

The cluster head plays the role of coordinator within its substructure. Each CH acts as a temporary base station within its cluster and communicates with other CHs.

A cluster is therefore composed of a cluster head, gateways and members node. Cluster Head (CH): it is the coordinator of the cluster. Gateway: is a common node between two or more clusters. Member Node (Ordinary nodes): is a node that is neither a CH nor gateway node. Each node belongs exclusively to a cluster independently of its neighbors that might reside in a different cluster.

3.2.1 Location Based Clustering

In the location-based routing protocol, the location information of mobile nodes are used to confine routing space into a smaller range .It reduces routing overhead and broadcast storm. The characteristics of Core Location-Aided Cluster-based Routing protocol (CLACR) are stated as the entire network is partitioned into square clusters.

In each cluster, the selection of cluster head is done by a cluster head election algorithm. The number of nodes responsible for routing and data transfer is decreased considerably by the usage of the cluster mechanism. It also diminished the routing overhead and increased the route lifetime massively. The path is computed using Dijkstra algorithm in a cluster-by-cluster basis by the CLACR.

3.2.2 Mobility Based Clustering

In a MANET node management is done by Clustering. Cluster formation: At first, a beacon message is send by each node to notify its presence to its neighbors. A beacon message contains the state of the node. A neighbor list is built by each node based on the received beacon messages. The cluster head is elected based on the weight values of the nodes.

The node with the lowest weight is chosen as the CH. Maintenance: It has two distinct types of operations like the battery power threshold property and the node movement to the outside of its cluster boundary. Mobility prediction: The improvement in the weighted clustering algorithm is due to the use of mobility prediction in the cluster maintenance phase.

3.2.3 Neighbor Based Clustering

In this scheme, the hierarchy is used to perform Route Discovery and distributes traffic among diverse multiple paths. Cluster Architecture: The CMDSR is based on the 3-level hierarchical scheme. The 0-node is the first level of the cluster. 1-cell cluster is the second level of cluster.

Here each node of the cell is 1-hop away from the Cluster Head. The 2-server cluster gathers a set of cells of which the Server is the leader. The cluster changes due to the nodal mobility dynamically. Hence the cluster will be disassembled or reassembled and also the cluster members update at every turn.

3.2.4 Power Based Clustering In

In this proposed new clustering algorithm, a stable clustering architecture is formed by defining a bottleneck node to be a node with battery power lower than a predefined value Threshold. Bottleneck cluster head refers to the bottleneck node elected as a cluster head.

The proposed clustering algorithm is based on the assumption that if the clustering architecture has fewer bottlenecks then the cluster heads have a longer lifetime.

3.2.5 Artificial Intelligence Based Clustering

The proposed mechanism selects the cluster head using fuzzy relevance for clustering in wireless mobile ad hoc sensor networks. In the network, the Fuzzy Relevance-based Cluster head selection Algorithm (FRCA) efficiently clusters and manages sensors using the fuzzy information of node status.

The Fuzzy Relevance Degree (FRD) with fuzzy value μ is used to perform and manage clustering in the proposed FRCA. In the proposed algorithm, some nodes acting as coordinators of the clustering are chosen by FRD to perform clustering.

3.2.6 File Searching

When a node initializes search for a file it sends a message FIND with its node id, requesting file name, data block of the file to the CH of its cluster. The CH searches its own MEMBER_INFO table for the requested file.

If it finds the file within its members, it sends ID of the node that contains the requested file to the requesting node. After this, requesting node goes for transferring the file from that node via CH.

When there remain multiple nodes with the same requested file, CH keeps track of that those alternate sources in its PATH table (TABLE 1). So in case of link failure the alternate path can be used to search the file or to transfer the remaining blocks of data. If the CH cannot find the requested file in its own cluster then it goes for inter cluster communication.

For this process, the CH broadcasts the FIND message on behalf of the requesting node to all of its member nodes. Upon receiving FIND messages from CH, member nodes of the cluster search for neighbouring nodes within their transmission range. The node checks out whether any of its neighbouring nodes is a member of different cluster and if so, then the FIND message is propagated to CH of another cluster through the neighbouring node.

When there reside no CH of different cluster within the transmission range of member node, the same process of broadcasting FIND message continues. For processing each query request within the cluster, CH initiates cluster update by sending and receiving HELLO to observe current status of its initial member nodes.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

Requesting Node ID	File Name	Requesting Data Block	Source Node ID	Next Node ID
1	A	0-7	2	5
1	A	0-7	3	6
1	A	0-7	5	7

Table: 3.1 Route table

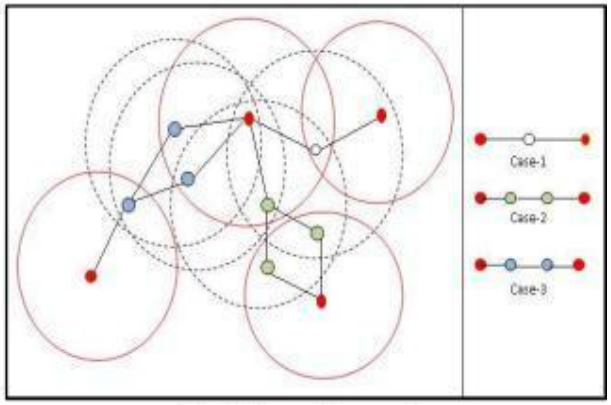

Figure 3.3 File Searching Scenario

3.3 CHALLENGES FOR CLUSTERING ALGORITHMS

Clustering in WSNs and MANETs no doubt has provided a number of advantages in deployment of routing protocols over the non clustering routing protocols. But it has to face several deployment challenges, such as

- Computing the optimal size clusters, traffic load distribution in clusters and the cluster stability.
- Ensuring connectivity.
- Selecting the appropriate CHs and the gateway nodes.
- Selecting the optimal frequency of CH rotation.
- Avoiding CH from becoming a bottleneck and single point of failure of the cluster.
- Optimal mode of communication between ordinary node and the CH.
- The control overhead of cluster construction and maintenance.
- Facing the network mobility and changes in the cluster structure frequently.

3.1 ROUTING ALGORITHM

The weight based routing algorithm is a position based routing algorithm where we assume that each node is equipped with GPS (Global Positioning System) which provides the location of the destination node and the node itself. The Routing Algorithm uses four types of packets:

- Hello Packets.
- RREQ Packets.
- RREP Packets.
- RRER Packets

The Routing Algorithm can be broadly divided into two phases:

1. Inter Cluster Routing
2. Intra Cluster Routing

3.1.1 Intra Cluster Routing

Cluster Head checks whether the destination node is within the Cluster or not .If the node is present within the cluster than the cluster head send the RREP reply packet with its ID embedded in the packet.

Now, the node forwards all the data packets required to be sent to the destination node to the cluster head which forwards to the destination.

3.1.2 Inter Cluster Routing

The node is present within the cluster then the cluster head forwards the packet to the destination node. If the node is not present within the same cluster then the cluster head finds the location of the destination from GPS and sends a RREQ packet to the gateway nodes in the direction of the destination.

- The destination is present within the Cluster of the Gateway nodes.
- The destination is not present within the Cluster of the Gateway nodes.

4. 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[4].

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

- 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.

4.1 Types of Clustering Approaches

The clustering categorized into different approaches based on the metrics considered for clustering. 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 are 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 poses 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.

5. CONCLUSION AND FUTURE ENHANCEMENT

5.1 Conclusion

MANET is one where there is no programmed infrastructure such as base stations or mobile switching centers. Key management in the ad hoc network is a difficult issue concerning the security of the group communication. In Mobile ad hoc networks (MANETs) security has become a primary requirement. The characteristics capabilities of MANETs expose both challenges and opportunities in achieving key security goals, such as confidentiality, access control, authentication, availability, integrity, and non-repudiation. Most cryptographic mechanisms, such as symmetric and asymmetric cryptography, often involve the use of cryptographic keys. However, all cryptographic techniques will be unsecure or inefficient if the key management is weak. Key management is also a central component in MANET security. The main purpose of key management is to provide secure methods for handling cryptographic keying algorithm. The proposed algorithm satisfies the scalability and mobility requirement by reducing the computational complexity of the algorithm. The results show that less computational overheads, average energy consumption and improves network lifetime and efficiency. Several aspects of MANET management can be included in the multi-objective optimization modeling approach proposed. Unlike most of the literature which focuses on one or two aspects of network management such as power management or routing efficiency, several goals can be defined in the proposed approach and optimized simultaneously through the clustering of network nodes. The contribution of the proposed procedure is that it presents a framework for including multiple criteria over which to cluster MANET nodes with the opportunity to prioritize various criteria through flexible logic rules.

In this research work initially various group key management schemes in both contributory and distributive are studied in all the aspects and comparison is provided. Even though many contributions and open problems are still available in the discussed schemes. In summary, improved Symmetric key management schemes are described in three categories DKPS, PIKE and INF. DKPS symmetric key management scheme is much efficient as compared to group key schemes and pair wise key agreement. PIKE scheme have good security services with fair scalability. INF model have no need of collaboration effort with having low storage cost. This paper concludes that DKPS is highly secure and efficient schemes as compared to other symmetric key management schemes.

Every type of asymmetric key scheme is described in a section 2. The identity-based key management is reliable and takes four phases, I, R, V and K which described in section 3. SEGK is group key scheme in MANET; double multicast tree is constructed in this model. Our cluster based enhanced group key management methods are useful to effectively transmit the data also provide secure data transmission over cluster heads.

5.2 FUTURE ENHANCEMENT

- Key management is crucial for MANET security. In future proposed to investigate network performance degradation due to such attacks when trust is used.
- Trust based cluster are formed based with routing considering intermediate nodes trust values. A control group generating the group key is proposed as a new technique in group key management.
- Cluster based key management scheme will be used heterogeneous network to manage network efficiency and reduce overhead ratio.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

REFERENCES

[1] I. Nishimura, T. Nagase, Y. Takehana and Y. Yoshioka, "Secure Clustering for Building Certificate Management Nodes in Ad-Hoc Network", International Conference on Network-Based Information Systems, (2011), pp. 685-689.

[2] H. Rifà-Pous and J. Herrera-Joancomartí, "A Fair and Secure Cluster Formation Process for Ad Hoc Networks", Journal Wireless Personal Communications: An International Journal archive, vol. 56, no. 3, (2011) February.

[3] V. Sivaranjani and D. Rajalakshmi, "Secure Cluster Head Election for Intrusion Detection in MANET", Journal of Computer Applications, vol. 5, Issue EICA2012-4, (2012) February 10.

[4] P. Goyal, S. Batra and A. Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications, vol. 9, (2010) November, pp. 11-15

[5] Yanchao Zhang ,Wei Liu, Wenjing Lou, and Yuguang Fang, "Securing Mobile Ad Hoc Networks with Certificateless Public Keys",IEEE Transactions on Dependable and Secure Computing, vol. 3,no. 4, OctoberDecember 2006.

[6] Chadi Maghmoumi, Hafid Abouaissa, Jaafar Gaber, and Pascal Lorenz, "A Clustering-Based Scalable Key Management Protocol for Ad Hoc Networks," Second International Conference on Communication Theory, Reliability, and Quality of Service, pp.42-45, 2009.

[7] Nen-Chung Wang, and Shian-Zhang Fang, "A hierarchical key management scheme for secure group communications in mobile ad hoc networks," Journal of Systems and Software, vol. 80, no. 10, pp. 1667-1677, 2007.

[8] Jin-Hee Cho, Kevin S. Chan and Ing-Ray Chen, "Composite Trust-based Public Key Management in Mobile Ad Hoc Networks".

[9] Rony H. Rahman, and Lutfar Rahman, "A New Group Key Management Protocol for Wireless Ad-Hoc Networks," International Journal of Computer and Information Science and Engineering, vol. 2, no. 2, pp. 74- 79, 2008.

[10] M. Bechler, H. -J. Hof, D. Kraft, F. Pählke, and L. Wolf, "A Cluster- Based Security Architecture for Ad Hoc Networks," Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM, vol. 4, pp. 2393-2403, 2004.

[11] Yi Jim Chen, Yi Ling Wang, Xian Ping Wu, and Phu Dung Le, "The Design of Cluster-based Group Key Management System in Wireless Networks," pp. 1-4, 2006.

[12] Jason H. Li, Renato Levy, Miao Yu, and Bobby Bhattacharjee, "A scalable key management and clustering scheme for ad hoc networks," Proceedings of the 1st international conference on Scalable information systems, 2006.

[13] J. Y. Yu and P. H. J. Chong, "A Survey of Clustering Schemes for Mobile Ad Hoc Networks", IEEE Communications Surveys & Tutorials, (2005).

[14] D. Wei and H. A. Chan, "Clustering Ad Hoc Networks: Schemes and Classifications", 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, (2006), pp. 920- 926.

[15] Hegland, A.M.; Winjum, E.; Mjolsnes, S.F.; Rong, C.; Kure, O.; Spilling, P.,"A survey of key management in ad hoc networks",IEEE,Communications Surveys & Tutorials, IEEE,2006