Efficient Group Key Management Protocol for Region Based MANETs

N. Vimala[*] B. Jayaram[@] Dr. R. Balasubramanian[#]

***Abstract*—Key management in the ad hoc network is an exigent issue concerning the security of the group communication. There are three categories for classifying Group key management protocols; centralized, decentralized and distributed. By establishing key management *protocol*, suitable solution can be provide to services like authentication, data integrity and data confidentiality. This paper deals with an approach for designing and analyzing the region-based Group key management protocols for scalable and reconfigurable group key management in Mobile Ad Hoc Networks (MANETs). The main issue of centralized key management protocols is about data security on group communication. To overcome this problem a novel approach for key management in Region based MANET is proposed. The Group key establishment comprises creating and distributing a common secret for all the group members. However, key management for a large and dynamic group is a difficult problem because of scalability and security. Modification of membership needs the group key to be refreshed to ensure backward and forward secrecy. In this paper, a Simple and Efficient Group Key (SERGK) management scheme is proposed for Region based MANETs. The proposed method is also effective in defending against many sophisticated attacks such as Denial of service (DoS) attack. In order to preserve the security, the region-based group key management protocols deal with outsider attacks in MANETs. The experimental results compares the computation cost and time for the existing and proposed approach and the results illustrate that the proposed approach outperforms the existing method with lesser computation cost and time.**

***Index Terms*—Cluster Head, Group Key, Key Management Protocol, Mobile Ad Hoc Networks (MANETs), Region-based and Rekeying**

I. Introduction

Basically, an ad hoc network is a collection of independent nodes which communicate with each other, most obviously by using a multi-hop wireless network. Nodes do not predictably know each other and come together to form an ad hoc network, only for some particular reason. Key distribution systems act as a trusted third party (TTP) that proceed as an intermediary between nodes of the network. A node has straight connection with a set of nodes, said to be neighboring nodes, in an ad hoc network which are in its communication range. The number of nodes in the network is not fundamental preset. Whenever the new nodes join the network, the older nodes are considered to be un-functional [1]. Key management in the ad hoc network is a main drawback, in terms of security of the group communication. The three categories for Group key management protocols are; centralized, decentralized, and distributed [2].

MANET has no predetermined infrastructure such as base stations or mobile switching centers (MSC). Wireless network plays a vital role in terms of communication; Mobile nodes can be communicated directly by means of a wireless network through radio waves, whereas those far apart rely on other nodes to act as routers to relay its messages [3]. The most suitable solution to provide the services among which authentication, data integrity and data confidentiality is the establishment of a key management protocol. Traffic encryption key (TEK) is used for generation and distribution of all the members in a group. This key is mainly favored by the source to encrypt multicast data and the receivers to decrypt it. Therefore legal members can only receive the multicast flow which is sent by the group source and other members are not allowed to receive the flow [4]. The key synchronism, secrecy, freshness, independence, authentication, and confirmation, forward and backward secrecy are the elemental security services provided by every key management system [7].

Cluster is eventually said to be group, while clustering is a phenomenon of collecting sub groups. Local controller (LC) is used to manage each sub-group, liable for local key management within its own cluster. Energy constitutes a foremost concern in ad hoc environments, moreover, not many solutions for multicast group clustering did think about the energy problem to realize an efficient key distribution process [5] [6]. Cluster head generates group key which communicate to other members through a secure and constrained channel that uses public key cryptography [14]. Clusters may be used for achieving different targets [8]. Clustering for transmission management, backbone formation, and for routing efficiency are some of ways for achieving different target. By outsiders and rouge members, group key management can be opposed to a broad range of attacks. In addition, group key management must be scalable, i.e., their protocols should be proficient in resource usage and able to decrease the effects of a membership change.

This paper proposes an approach for the design and analysis of region-based key management protocols for scalable and reconfigurable group key management in MANETs. The proposed approach describes about the simple and efficient group key (SERGK) management for region based MANETs. Group key establishment refers that multiple parties want to create a common secret to be used to exchange information securely. Without depending on a central trusted entity, two people who do not previously

[*] Senior Lecturer, Department of Computer Science, CMS College of Science and Commerce, Coimbatore, India.

[@] Asst.Proffessor,Department of Computer Science & Engineering, PA College of Engineering and Technology,Pollachi,Coimbatore,India

[#] Dean Academic Affairs, PPG Institute of Technology, Coimbatore, India

share a common secret can create one based on the DH protocol. The 2-party Diffie-Hellman (DH) protocol can be extended to a generalized version of n-party DH. Research efforts have been put into the design of a group key management scheme for the sake of scalability, reliability, and security. Furthermore, group key management also needs to address the security issue related to membership changes. The modification of membership requires refreshment of the group key. This can be done either by periodic rekeying or updating right after member change. The change of group key ensures backward and forward security.

In this paper, a simple and efficient region based group key management scheme is proposed, simply called SERGK, for MANETs. The basic idea of SERGK is that a physical multicast tree is formed in MANETs for efficiency. Group members take turns acting as group coordinator to compute and distribute intermediate key materials to group members. The keying materials are delivered through the tree links. The coordinator is also responsible for maintaining the connection of the multicast group. All group members can calculate the group key locally in a distributed manner.

The rest of this paper is structured as follows. Section II of this paper discusses some of the proposed cluster based group key management techniques. Section III describes our proposed method of new region based simple and efficient group key management protocol for MANETs. Section IV explains the performance evaluation of the proposed approach and section V concludes the paper with fewer discussions.

II. Background Study

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

Maghmoumi et al. in [9] put fourth 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 affinity 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 [10]. 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.

George et al. in [11] gave a new thought about framework for key management that provides redundancy and robustness for Security Association (SA) establishment between pairs of nodes in MANETs. They have worn a modified hierarchical trust Public Key Infrastructure (PKI), which nodes can keenly assume management roles. Furthermore they employed non-repudiation through a series of communication checks to securely communicate new nodes information among Certificate Authorities (CAs). They unsaid that nodes could leave and join the network at any time. Nodes could generate their own cryptographic keys and were proficient of securing communication with other nodes. In order to poise the flexibility and increased availability of the Key Management Scheme (KMS), security was provided by introducing two concepts in addition to revocation and security alerts: non-repudiation and behavior grading. The KMS determined sufficient levels of security by combining node authentication with an additional element, node behavior. A behavior grading scheme is essential each node to grade the behavior of other nodes.

A new group key management protocol for wireless communication ad hoc networks was stated by Rony et al. in [12]. 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, 'K,' 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. The password 'P' is also most common among each valid member present in the scenario. This 'P' helps for authentication process and prevents man-in-the-middle attack. Unlike several other protocols, the proposed approach does not need broadcast/multicast capability.

Bechler et al. in [13] proposed cluster-based security architecture for Ad hoc networks. They proposed and predictable 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. The architecture addresses problems of authorization and access control, and a multi-level security model helps to adjust the complexity to the capabilities of mobile end systems. Based upon their authentication infrastructure, they afford a multi level security model ensuring authentication, integrity, and confidentiality.

A scalable key management and clustering scheme was anticipated by Jason et al. in [15]. 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 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.

Apart from the above mentioned numerous researches; they have been conducted in the field of cluster-based group key management for mobile ad hoc networks (MANETs).

III. Methodology

3.1. New Region Based Group Key Management for MANETs

The region-based group key management protocol segregate a group into region-based subgroups based on decentralized key management principles. This separation of region into subgroups improves scalability and efficiency of the key management scheme in providing a secure group communication.

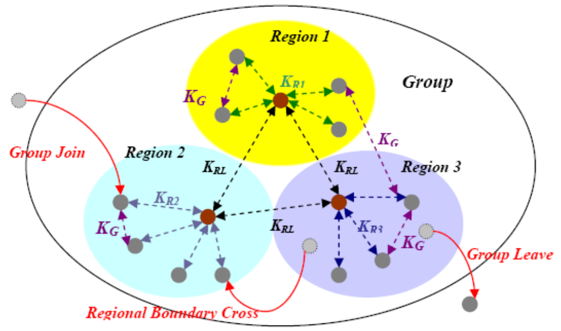


Figure 1. Region-based Group Key Management

Figure 1 shows that the partitioning of region into subgroups on the basis of decentralized key management principles [16]. It is assumed that each member of the group is set up with Global Positioning System (GPS) and therefore each one knows its position as it moves across the regions. In secure group communications, all members of a group carve up a secret group key, K_G. In addition to guarantee the security in communication between the members of each subgroup all the members of the subgroups in the region 'i' hold a secret key K_{Ri}. This shared secret key is engendered and managed by a distributed group key management protocol that enhances robustness. This region-based group key management protocol will role up at the optimal regional size recognized to reduce the cost of key management in terms of network traffic.

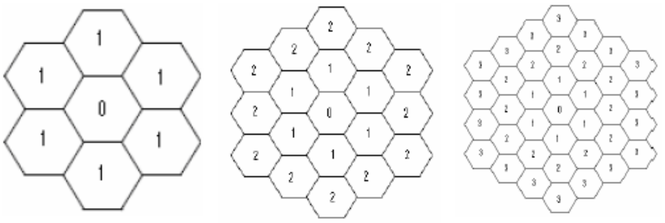
N=λ_pA, the average number of nodes in the system, where λ_p denotes the node density of the randomly distributed nodes and A point out the operational area with radius 'r'. The random distribution of nodes is dependent to a homogeneous spatial Poisson process. The nodes that can either join or leave a group at instant point of time. A node may disappear from a group at any time with rate μ and may rejoin any group with rate λ. Therefore, λ/(λ+μ) is the probability that a node is in any group and the probability that it is not in any group is μ / (λ+μ). Let A_J and A_L be the group that join and leave rates of all nodes, respectively.

Then, A_J and A_L, can be calculated as follows,

$$A_J = \lambda \times N \times \frac{\mu}{(\lambda+\mu)}$$

$$A_L = \mu \times N \times \frac{\lambda}{\lambda+\mu}$$

Nodes in a group must suit the forward/backward secrecy, confidentiality, integrity and authentication necessities for secure group communications in the presence of malicious outside attackers. The important obligation for secure group communication is reliable transmission. This can be complete by using acknowledgement (ACK) packets and packet retransmission upon timeout. Hexagon is used to model a region [17]. Let R(n) denote the number of regions (i.e. $3n^2 + 3n + 1$) in the operational area. For n=3, the number of regions in the operational area is 37, for n=2 and n=1, the number of selected region in operational area are 19 and 7 respectively. Figure 2 shows the pictorial representation of the regions in the operational area for n=1, 2, and 3.



n=1, Number of Regions=7 **n=2, Number of Regions=19** **n=3, Number of Regions=37**

Figure 2. Representation of Regions in operational area

A. Protocol Description

This describes the working of our proposed region-based group key management for MANETs.

1. Bootstrapping

In this primary bootstrapping process, a node surrounded by a region can take the dependability of a regional "leader" to carry out Group Diffie Hellman (GDH). If there are numerous initiators, then the node with the smallest ID will exist as the leader and will implement GDH to completion to generate a regional key. Once a leader is engender in each region, all leaders in the group will execute GDH to agree on a secret leader key, K_{RL}, for secure communications among leaders. The group key K_G can be created using the following, K_G = MAC (K_{RL}, c), where MAC is a cryptographically secure hash function, K_{RL} is the leader key used as the secret key to MAC, and c is a fresh counter which will be incremented whenever a group membership event occurs. The generated group key K_G is then dispersed among the group members by the group leader. This group key affords secure group communication across regions.

2. Key Management

The next important task is managing the generated key. These collective secret keys at the subgroup (regional), leader, group levels may be rekeyed to preserve secrecy in response to events that occur in the system. Therefore, whenever there take place a change in the leader of the group, the leader key, K_{RL} is rekeyed. The regional key (K_R) is rekeyed at any time there is a regional membership change, including a local member group join/leave, a node failure, a local regional boundary crossing, and a group merge or partition event.

3. View Management

In addition to maintaining secrecy, the proposed region-based key management protocol also allows membership consistency to be maintained through membership views. Three membership sights can be maintained by various parties: (a) Regional View (RV) contains regional membership information including regional (or subgroup) members' ids and their location information, (b) Leader View (LV) contains leaders' ids and their location information, and (c) Group View (GV) contains group membership information that includes members' ids and their location information.

3.2. Simple Efficient Region based Group Key Management

The simple and efficient region based group key management (SERGK) scheme is presented as follows

3.2.1. Notations and assumptions

It is assumed that a valid certificate from offline configuration is carried by every node before entering the network. A smart card can be used for this pre-configuration. Therefore, there is an underlying public key infrastructure to manage certificates. When referring to the literature, most solutions suffer the man-in-the-middle attack. In this proposed approach, it is assumed that each group member has a unique identifier and all keying materials are digitally signed by corresponding initiators to ensure authenticity and integrity, and to defend against man-in-the-middle attacks. The group access control depends on the group membership policy. A member can carry some secret information (such as a password) in order to join the group or a node can join a group if it can present a valid certificate, etc. Here, for simplicity, it is assumed that a node can join a group if it has a valid certificate. Some notations used in SERGK are listed in TableI.

TABLE I SOME NOTATIONS USED IN SERGK SCHEME

M_i	A group member with ID i
M_c	The current group coordinator
n	Total number of group members
g	Exponentiation base
r_i	a random number generated by member i, also called member key
br_i	Member i's blinded member key, bri = gri mod p
k_i	Internal node i's key, ki = $(br_i)^{ki}$, also called intermediate key
bk_i	Blinded internal node i's key, bk_i = g^{k_i}= , also called blinded intermediate key
h(m)	The digest of m
K_G	The common group key

3.2.2. Key Management by SERGK approach

Every group member contributes a share of the final common group key, to form a common group key in the proposed approach. The group key can be refreshed periodically or only be updated in response to changes of group membership. The updating of the group key helps to enforce backward and forward secrecy of group communications. Obviously, efficiently exchanging keying materials is critical in MANETs. In SERGK, all keying materials are disseminated through the underlying multicast tree links. A native broadcast through flooding is obviously not appropriate because of large redundancy which may result in network traffic congestion. There are many multicast routing protocols that have been proposed, and they are described in Section 2. Here, a reliable double multicast tree formation and maintenance protocol is presented. This idea is similar to Wei and Zakhor [18], however, the double tree scheme guarantees that two trees cover all group members. Logically, the two trees are identical from a group member's point of view. In Wei and Zakhor (2004), some group members included in one tree might not be included in the other tree, which is obviously not desirable for group key management. The multicast routing protocol serves as a subsystem of our group key management framework. The detailed protocols are presented as follows.

Group initialization process is started by a group initiator by broadcasting a join advertise message across the entire network. A sequence number is used to avoid loops. A node is coupled with three colors, namely blue, red, and grey. A node will choose grey as its color if its total number of neighbours is less than a predefined threshold value (for instance, half of average node degree). All member nodes are grey. Other network nodes randomly choose blue or red as their color with probability equal to 0.5. For the first received message, a grey node stores the upstream node ID and rebroadcasts the message. For a non-grey node, it stores the upstream node ID and rebroadcasts the message only if the upstream node is the same colour, a sender, or a grey node. Based on the join response back from group member to the group initiator, two double multicast trees are formed in parallel. Both trees consist of group members and intermediate non-member nodes. A node could send out join requests to a group. Any existing group member can send replies back. The procedure of handling join requests is similar to the above group advertisement to ensure the consistency of double multicast tree structures. The resultant two trees could be disjoint or may share a common node. Thus, a dynamic double multicast tree structure is constructed. Figure 3 illustrates the construction of a double multicast tree.

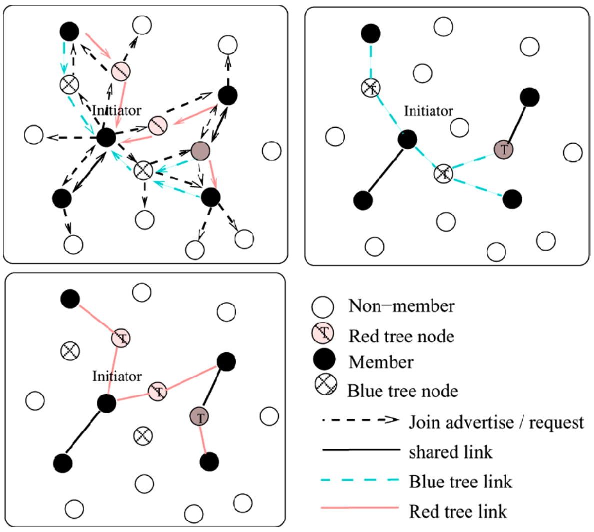


Figure 3 Illustration of a double multicast tree structure

3.1.1. Construction of double multicast trees

The above approach met with a problem, which is that the two multicast trees may not be identical, which means some group members may be covered by the blue tree, but are not included in the red tree. This scenario can happen when a group member is surrounded by nodes with only one colour, either red or blue. A group member can detect this scenario if it has received messages from only one colour (either blue or red) of nodes. Then, this member node can request one of its upstream nodes to change its colour to grey.

The group initiator is responsible initially, for sending out member refresh messages periodically to maintain the connection of the double multicast tree structure. After an amount of time of operation which is predefined, a group member could decide to act as a group coordinator and notify the group that it is on duty to maintain the group. All members need to take turns acting as group coordinator. The double multicast trees can be used by enabling one tree in an active state and the other one in an inactive state as a backup. After a predetermined period of time for the group initialization phase, the multicast trees have been formed and the group coordinator can invoke the group key establishment procedure. This procedure is described in detail in the group key establishment.

3.2.3. Detection of leaving members

It is more complicated to handle the member leaving than handling the joining of new members. To join the group, a new user needs to broadcast a request. The new user becomes a legitimate group member once its request is approved by any existing group member or by the current group coordinator. However, for the scenario of leaving members, it cannot be assumed that a leaving member will send out a leaving notice. A member could leave the group silently. Even if it could send out a message and notify its leaving, this notice could get lost in a dynamic environment. A physical leaving and a logical leaving can be defined. For the physical leaving, a node moves out the range of the network or it switches its transmitter off. For a logical leaving, a node still stays inside the network, but it does not participate in the group activity. Two methods are presented to address these problems.

A. Method one

The first method's strategy is that current group coordinator sends out member refresh messages periodically through both tree links. All group members should send an ack message back to indicate its affiliation interests (status). The group coordinator will determine whether a member remains attached or has left based on its response within a certain amount of time. It is the member's responsibility to broadcast a message in a controlled flooding scheme to reconnect to the group if it has not heard the periodic member refresh message. If a member does not want to be part of the group it could keep silent without sending the ack message. The tree structure is updated based on the control messages. Some links could be pruned and new links could be added since a member could move to a new location. The current group coordinator notifies the member change event to all members through the updated tree structure. This strategy is very efficient and is appropriate for a relatively static network environment.

B. Method two

The second method has another strategy is that the group initiator or current group coordinator periodically broadcasts member enforcement messages in a controlled flooding scheme. The default flooding range is set to the maximum distance from the coordinator to the members. The search range can be increased until it reaches a threshold value or the current network diameter. All group members will send a response back. Thus, members affiliated to the group are refreshed. This strategy is quite costly compared with Method one, and is more appropriate for a highly dynamic environment where nodes move frequently and cause the connections to be broken frequently.

3.2.4. Group key establishment protocol

The core idea of a group key agreement protocol is that all group members maintain a logic key tree in local storage space. The key tree is used to deduce the final common group secret. Most contributory group key approaches maintain a certain type of key repository. They differ in the way they accumulate and distribute intermediate keys. Some are based on the key ring and the others may be based on key tree, etc. The proposed scheme is based on the key tree structure. Although the proposed key tree is similar to STR, several improvements are introduced as describe below. The key tree structure in SERGK is shown in Figure 4.

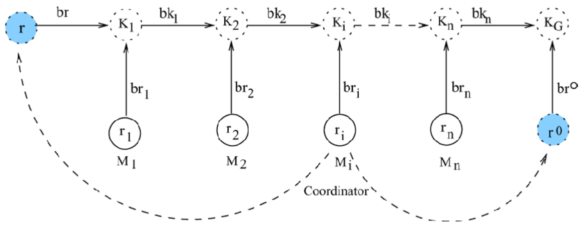


Figure 4 Illustration of key tree structure

- To distribute the workload of keying service, the concept of coordinator is introduced. The coordinator is responsible for computing and distributing intermediate keys to all group members. It also needs to handle member join and leave. The role of coordinator is rotated among all members.
- For efficient switching of the role of coordinator, two dummy nodes at two ends of the key tree are introduced for efficient group key refreshing and the group coordinator role switching.
- A new group member can be easily absorbed into the group by adding new members into the current rightmost position and moving itself to the right.
- When a member leave is detected, the coordinator generates a new random key r and multicast the blinded value b_r as well as other intermediate blinded keys.

A. *Group key initialization*

The coordinator announces its role and broadcasts two random keys r and r_o, at the initialization phase. Normally the group initiator acts as group coordinator at the beginning. The order of members on the key tree is sorted by their ID at the initialization phase. However, at subsequent member add events, a new member is always added at the rightmost position of the key tree. This rule should be followed by all members to ensure that key trees in all members' local memory are consistent. One solution is that the group coordinator explicitly indicates the structure of the key tree. This can also be done implicitly by the coordinator since it needs to multicast blinded intermediate keying materials to all group members. All keying materials are put in one package and the order of blinded intermediate key materials shows the structure of the key tree.

B. *Member addition*

A new group member can be easily added into the group by inserting it into the current rightmost position and moving the dummy coordinator to the right. The major advantage of this approach is that the coordinator does not need to generate a new random key but still provides key independence. This means that knowing the previous group key cannot help to deduce the new group key. Given two blinded keys, the new member can deduce the new group key, however, it cannot deduce the former group key. This ensures backward secrecy. Figure 5 illustrates the operation of joining a new member.

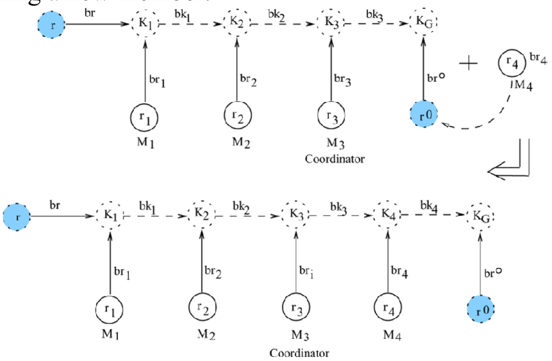


Figure 5 Illustration of key updating for joining member

C. *Member leave*

The leaving group member event can be detected either by explicit notification from the leaving node or through the scheme described before through Method one or Method two. The coordinator notifies all group members of the member leaving event and multicasts a new blinded random key to all members. All group members can compute the new group key. Figure 6 illustrates the operation of a leaving member.

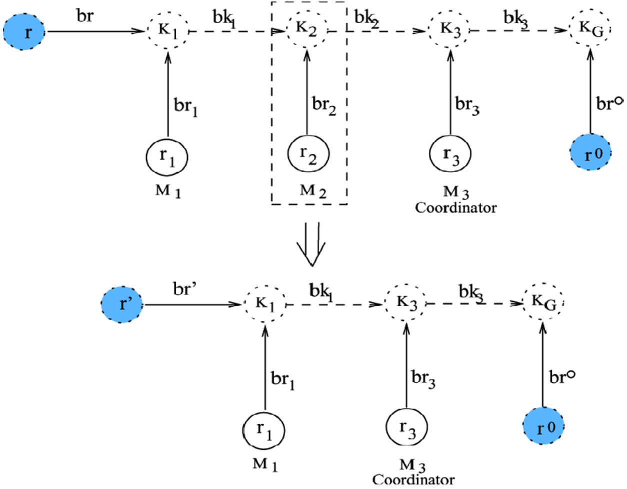


Figure 6 Illustration of key updating for leaving member

IV. Performance Analysis

The performance analysis helps to recognize the optimal regional size that will minimize the network traffic generated while satisfying security properties in terms of secrecy, availability and survivability. The cost metric worn for measuring the proposed group key management protocol is the total network traffic per time unit incurred in response to group key management events including regional mobility induced, group join/leave, periodic beaconing, and group merge/partition events. To calculate the performance of this proposed approach join/leave cost, and group communication cost are discussed on a group.

The simulation was implemented in NS2. The simulation was conducted in a 100 × 100 2-D free-space by randomly allocating a given number of nodes in the range from 50 to 200. A dynamic network environment is used to conduct the experiment. It is assumed that every node has fixed transmission range r = 20. If their distance is within each other's transmission range, two nodes are directly connected. For each host in an update interval, the corresponding host may move within the range of l units in any direction or remain stable in the corresponding internal with the possibility ρ (l is 5 and ρ is 0.5 in this simulation). The results are compared with some of the proposed distributed approaches and ignore other centralized approaches. In this experiment, the cost of SERGK with the existing RGK scheme is compared. 1024-bit prime number is taken as random key. A base g = 2 with the module n (1024 bits) is used to compute the blinded random key as well as the blinded intermediate keys. A time stamp, sequence number, flags, and keying materials are concatenated and hashed using MD5 (256 bit), and then signed by the senders' private key.

4.1. Cost measurement

In the experiments, the cost is measured both by the number of messages and the computation time. For the SERGK scheme, the message cost includes the multicast of blinded random keys and the intermediatory keying materials. The multicast tree nodes include all group members as well as non-group forwarding nodes needed to forward messages. Every forwarded message is counted. The message cost for the group key initialization process and for member joining and leaving scenarios are analyzed. For the RGK scheme, the message cost includes the flooding of all blinded keying materials, which includes random keys and intermediatory keys. The computation cost mainly includes generating large prime numbers, performing exponentiations, hashing, and producing signatures. The experimental observations of the computation cost when p=10% are presented in figure 7.

The figure clearly shows that the average message cost of the SERGK is lesser than the RGK approach. This shows that the proposed approach performs better than the previous region based group key management techniques. The performance of the system can be assed with the computation

Time and the comparison of computation time for the two approaches are given in figure 8. The time taken by the present RGK and the proposed SERGK approach are compared in the figure 8.

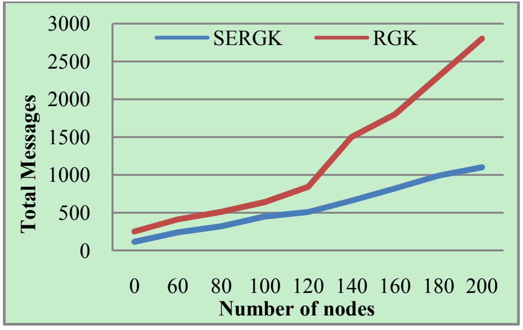


Figure 7 Comparison of Average message cost for SERGK and RGK when p=10%

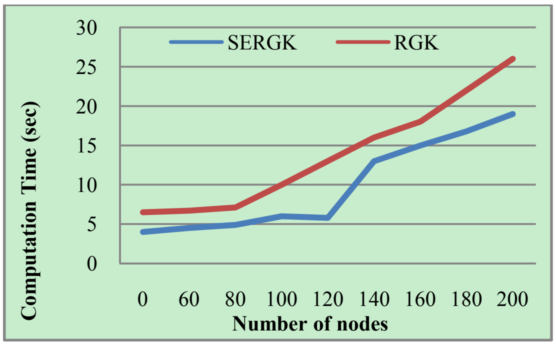


Figure 8 Comparison of Average computation time for SERGK and RGK when p=10%

The figure clearly illustrate that the proposed approach uses only less computation time than the present RGK approach.

V. 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. This paper gave an approach for the design and analysis of region-based key management protocols for scalable and reconfigurable group key management in MANETs. The proposed simple efficient region-based group key management protocol divides a group into region-based subgroups based on decentralized key management principles by using the efficient Region based group key management Protocol (SERGK). In this approach, there is one group member that acts as a group coordinator which computes and distributes the blinded intermediate keying information the group. Every member computes the group key in a distributed manner. To distribute the workload of group rekeying and maintenance, the role of group coordinator is rotated among all members. A new key tree structure is introduced in order to switch the group control role efficiently. A simulation study has been conducted to compare the message cost and computation cost under group key management schemes and it is found that the proposed approach performs better than the present RGK approach.

References

[1] A. Renuka, and K. C. Shet, "Cluster Based Group Key Management in Mobile Ad hoc Networks," IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 4, pp. 42-49, 2009.

[2] S. Rafaeli, and D. Hutchison, "A survey of key management for secure group communication," ACM Computing Surveys, vol. 35, no. 3, pp. 309–329, 2003.

[3] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang, "Security in mobile Ad-Hoc networks-Challenges and Solutions," IEEE Transactions on Wireless Communications, vol. 11, no. 1, pp. 38-47, 2004.

[4] Mohamed-Salah Bouassida, Isabelle Chrisment, and Olivier Festor, "Group Key Management in MANETs," International Journal of Network Security, vol. 6, no. 1, pp. 67-79, 2008.

[5] L. Lazos, and R. Poovendram, "Energy-aware secure multicast communication in Ad Hoc networks using geographical location information," in IEEE International Conference on Acoustics Speech and Signal Processing, pp. 201-204, 2003.

[6] J. E. Wieselthier, G. D. Nguyen, and A. Ephremides, "On the construction of energy-efficient broadcast and multicast trees in wireless networks," in INFOCOM 2000, pp. 585-594, 2000.

[7] Menezes, P. V. Oorschot, and S. A. Vanstone, "handbook of Applied Cryptography", CRC Press, New York, 1997.

[8] C. E. Perkins, "Ad hoc networking", Addison-Wesley Pub Co, 1st edition December 29, 2000.

[9] 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.

[10] 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.

[11] George C. Hadjichristofi, William J. Adams, and Nathaniel J. Davis, "A Framework for Key Management in Mobile Ad Hoc Networks," International Journal of Information Technology, vol. 11, no. 2, pp. 31-61, 2006.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] Jin-Hee Cho, “Design and Analysis of QoS-Aware Key Management and Intrusion Detection Protocols for Secure Mobile Group Communications in Wireless Networks,” Thesis submitted to the Faculty of the Virginia Polytechnic Institute and State University.

[17] J. W. Wilson, and I. R. Chen, “Performance Characteristics of Location-based Group Membership and Data Consistency Algorithms in Mobile Ad hoc Networks,” International Journal of Wireless and Mobile Computing, vol. 1, no. 8, 2005.

[18] Wei, W. and Zakhor, A. (2004) ‘Conectivity for multiple multicast trees schemes in ad hoc networks’, International Workshop on Wireless Ad Hoc Networks (IWWAN 2004), Oulu, Finland, pp.270–274.

N. Vimala received her B.Sc., (CS) from Avinashilingam Deemed University, Coimbatore, TamilNadu, in 1993. She obtained her M.Sc., (CS) and M.Phil degree from Bharathiar University, Coimbatore, TamilNadu, in the year 1995 and 2001 respectively. She is currently the Senior Lecturer, Department of Computer Science, CMS College of Science and Commerce, Coimbatore, TamilNadu. She has the long experience of teaching Post graduate and Graduate Students. She has produced 43 M.Phil Scholars in various universities. Her area of interest includes Network Security, Database Management Systems, Object Oriented Programming and Artificial Intelligence. She is currently pursuing her Research in the area of Network Security under Mother Teresa University, Kodaikanal, TamilNadu. She is a member various professional bodies.

B. Jayaram obtained his M.E in Computer Science and Engineering in the year 2006 from Anna University, Chennai. He is currently working as Assistant Professor, Department of Computer Science & Engineering, PA College of Engineering and Technology, Pollachi. He has previously served as lecturer prior to this he had served as an active member of the development team in ERP products at Ramco Systems, Chennai. His area of interest includes data structure, computer networks, data mining, and biometrics.

Dr. R. Balasubramanian was born in 1947 in India. He obtained his B.Sc., and M.Sc., degree in Mathematics from Government Arts College, Coimbatore, TamilNadu, in 1967 and PSG Arts College, Coimbatore, TamilNadu, in 1969 respectively. He received his Ph.D., from PSG College of Technology, Coimbatore, TamilNadu, in the year 1990. He has published more than 15 research papers in national and international journals. He has been serving engineering educational service for the past four decades. He was formerly in PSG College of Technology, Coimbatore as Assistant Professor in the Department of Mathematics and Computer Applications. He served as Associate Dean of the Department of Computer Applications of Sri Krishna College of Engineering and Technology, Coimbatore. Currently taken charge as Dean Academic Affairs at PPG Institute of Technology, Coimbatore, before which he was a Dean Basic Sciences at Velammal Engineering College, Chennai. He has supervised one PhD thesis in Mathematics and supervising four doctoral works in Computer Applications. His mission is to impart quality, concept oriented education and mould younger generation.

He is member of the board of studies of many autonomous institutions and universities. He was the principal investigator of UGC sponsored research project. He is a referee of an international journal on mathematical modeling. He has authored a series of books on Engineering Mathematics and Computer Science. He is a life member of many professional bodies like ISTE, ISTAM and CSI.