Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 5, April-2019, ISSN 2230-7540

An Efficient Group Key Management Protocol

Tilak Singh Rajput[1]* Dr. Satendra Kuraria[2]

[1] Research Scholar, Department of Computer Science, Sri Satya Sai University of Technology & Medical Sciences, Sehore, M.P.

[2] Research Guide, Department of Computer Science, Sri Satya Sai University of Technology & Medical Sciences, Sehore, M.P.

Abstract – Multicasting is a process of transmitting a message from one sender too many receivers or from several senders to multiple receivers. If there is a need to send the similar message to several destinations, then multicast is the most ideal choice than the multiple unicast. The major advantage of using multicast is that, it facilitates the preferred applications to service many users without any congestion in the network and resources in the server. In this paper, we propose a novel, secure, scalable and efficient Region-Based Group Key Agreement protocol SERGK for ad-hoc networks.

Key Words: Ad Hoc Network, Region-Based Group Key Agreement Protocol.

----------X----------

1. INTRODUCTION

Wireless network is a kind of computer network that is wireless that is usually linked with telephone network and the interconnections between nodes are connected without using any wires. The realization of wireless telecommunication networks will be for some kind of remote information communication device that utilizes electromagnetic waves, including radio waves, for the carrier of information and this way of application usually takes place at the physical level or layer of the network.

Most wireless networks operate on the IEEE 802.11 standards [1]. The fundamental network consists of multiple stations communicating with radios that broadcast in either the 2.4GHz or 5GHz band (despite the fact that this varies due to the circumstances and is also changing to allow contact in the 2.3GHz and 4.9GHz ranges).

2. SECURITY ISSUES IN MULTICAST

Security is necessary for data transmission in an unconfident network. There are number of approaches to deal with the unicast security concerns but they cannot directly be extended to a multicast atmosphere. On the whole, multicasting is extremely more susceptible [2] than compared with the unicast network because the transmission occurs over multiple network channels. A more dynamic and daunting challenge occurs since the membership of the multicast community is lively. Users are able to leave and join the groups, which makes group management of large-scale structures more challenging.

In addition, confidentiality and backward security must be given. Further confidentiality ensures that any time a member of a group leaves the group, no one in that group should be able to hear more talk. Backward confidentiality means that a new party is not expected to be allowed to view past talks of that party. Multicasting covers both real-time and non-real-time programmes. If these difficulties are not identified effectively, a severe bottleneck may be developed, especially in real-time applications like VoIP systems.

It is also absolutely necessary for a protection system used in a multi-cast setting not only to be protected but also to be very competent to reduce these bottlenecks.

One of the big multi-cast protection problems is the GKM. Many multicasting authentication schemes have been developed and can usually be divided into two specific categories.

- Centralized Scheme
- Distributed Scheme

GKM is applied by the System Controller (GC) for the centralised process, and there is no difficulty for group users. Every consumer carries out the necessary operations for GKM in the second

scheme. Consequently, the consumers have extra burdens.

In unicast communication the protection is provided by encrypting the message on the sender's side with the aid of a key and by decrypting with the recipient's similar key. A similar approach is taken in securing the multicast community. The entire party shares a key called the Session Encryption Key (SEK), which is only known by legitimate group members. The mutual key is used to encrypt every message within the party. The SEK is used by all the participants participating in this group to encrypt group session messages. Whenever the party membership adjusts, the SEK has to be restructured. And to prevent fresh members deciphering recent talks, avoid members that have quit to decipher potential talks.

3. REVIEW OF LITERATURE

Qiuna Niu [3] suggests a distributed, group-oriented key management system without the intervention of third parties. Compared to standard Diffie-Hellman, the scheme uses Elliptic Curve Diffie-Hellman (ECDH), which is lighter. The technique involves group core establishment and rekeying algorithms as changes in composition arise. The load of main management is minimised by using a distributed architecture. Specifically, to have greater scalability, the scheme can be generalised to hybrid architecture. Consequently, in terms of honesty and secrecy, the expanded framework is both fault-tolerant and efficient. The mutual group key is determined by scalar multiplication in all protocol suites. The suggested method significantly lowers communication overhead and computing costs according to efficiency comparisons with other systems. Security research reveals that a range of attractive security features are offered by the initiative, including community key confidentiality, forward secrecy and backward secrecy.

Priyanka Ahlawat [4] provides a thorough analysis of the latest state-of-the-art WSN protection KMS and contrasts it with many measurement criteria. Based on current literature reviews, they also investigates the protection criteria, priorities and difficulties of KMS. They are also seeking to provide insight into future research developments in the field of WSN security and detail the methods that are expected to play a very important role. Therefore, for WSN stability, the methods of reliable allocation and management of these keys are very important. In recent years, several KMSs have been created. However, WSN's inherent features make it a major challenge to integrate security.

Renu Dalal et. al. [5], presented the analysis with its special features on different types of main management systems. the mobile Ad-hoc network is random and the network consists of cellular mobile nodes with fewer infrastructure. MANET is formed on-the-fly and also offers different operations between mobile nodes, such as packet forwarding, routing, network control, connectivity, etc. MANET is one of the types of wireless network in which, during a complex time, any mobile node will enter the network and exit the network. In order to achieve a safe environment, various trust mechanisms are used to provide security, credibility and connectivity in the mobile ad-hoc network.

Ayman EL-SAYED [6], a new group key management scheme is introduced in this article, namely a Hierarchical, Simple, Effective and Scalable Group Key (HSESGK) based on the MANET clustering management scheme and numerous other schemes are classified. In a dispersed way, group members subtract the group key. Providing a key control protocol is the most effective way to provide these facilities with the expected degree of protection. Key control is an integral aspect of protection. In the cellular network, this dilemma is much stronger relative to the wired network. In MANET, the delivery of keys in an authenticated way is a challenging task. It needs to create a new key to preserve forward and backward confidentiality when a member leaves or joins the party.

M. El-Bashary et. al [7], stated that Mobile Ad-Hoc Network (MANET) is a self-organized network with minimal funding, limited physical protections, and no fixed infrastructure. An integral necessity is protection in such a setting. In MANET security, key management is a prominent feature. Key generation, collection, delivery, upgrading, revocation, deletion, and archiving are responsible for it. Main protocols for management are grouped into symmetric, asymmetric, group, and hybrid. Community main control for researchers with the use of mobile devices and the use of multicast communication is a topic of concern. In community core management systems, this paper surveys numerous approaches. In terms of durability, computing complexity, storage costs, connectivity overheads, pre-requirements, protection thresholds, robustness, weaknesses, scalability, energy and agility, a comparative analysis has been shown. Finally, the report concludes that the pros and cons of each protocol are.

4. GROUP KEYING

Several Internet technologies have been developed, such as digital video distribution on the pay-per - view side, selective teleconferences, shared games and simple private networks. In certain models, group members can use the same symmetrical key, known as a group key that is only recognised by the group users and the key server. The group key can be used to encrypt data collisions

between group members or to control access to services for group members only.

The group key is disseminated through a GKM system, which sometimes transforms the group key called group rekeying. The group key has to be converted as a result of connection by a new user (to guarantee that the new user is unable to decode previous group communications), or the current user leaves the group (to prohibit departing users from accessing future group communications).

A GKM framework has three useful registration, key management and rekey transportation processes. You will perform all three mechanisms on a main server. On the other hand, it is easier to use one or more trustworthy registrar to boost registration scalability in order to eliminate user registration from the main server.

If a user wants to be connected to a group, the user and the registry system often validate one another with a Stable Sockets Layer (SSL) protocol. When authenticated and integrated in the community, the new user gets its identity and a symmetric key, called the individual key of the user, which it only shares with the key server. Authenticated users move on the request to the key management component, validating whether they are encrypted using individual keys to authenticate requests. The key management mechanism often creates rekey messages that are passed to the rekey transportation mechanism to all users in the group. In order to develop a scalable GKM infrastructure, the efficacy of the main management and reclamation processes must be enhanced.

The rekey transport part is then taken into account. In current works, reliable distribution of rekey messages had no thought. This thesis also analyses the efficiency difficulties of rekey transportation and finds that many multi-cast protocols are currently accessible and tested. The rekey transport varies in many ways from conventional stable multicast problems. Rekey transport has the following necessities in total:

- *Consistency Requirement*: It is important, without considering the community size, for each user to get all their encrypted new keys. This need exists because the key server requires some keys for the next rekey interval to encrypt new keys. In the other side, each user does not have to receive the entire key message since all new keys are split very small.

- *Soft Real-Time Requirement:* It is essential that the release of new keys to all users be completed with a better probability prior to the establishment of the subsequent rekey interval. This condition arises since a user desires to buffer encrypted data and keys prior to the appearance of encrypting keys and the buffer size is inadequate.

- *Scalability Requirement:* Handling bandwidth necessities of the key server, each user is supposed to increase as a function of group size at a small rate such that a single server is capable of managing a large group.

5. GROUP KEY DISTRIBUTION SCHEMES

The Group Key Management Protocol (GKMP)[8] is a Group Key Management Structure (GKM) for the purpose of multi-cast Internet security. This is completely different from the Single Key Distribution Center (SKDC) schemes, and GMKP is not allowed to exist as a member of the community in a third party KDC. GKMP, on the other hand, retains a key institution by pair exchange. Certain aspects of the GKMP approach in the alternative receiver started are that a GKC multicast or party key manager is picked by vote; keys have an insufficient time life. GKC generates community key packets while other servers produce multicast encrypted traffic. However, provided that the current group key is encrypted from an open group-wide KEK, forward security is not conserved. An entirely new community must be created to prevent compromise.

The Logical Main Hierarchy (LKH)[9, 10, 11] is one of many approaches to virtual hierarchical tree topology. In LKH, all the leaf-node of a binary tree retains KEKs of these nodes along a shorter path from the leaf to the root corresponding to the GKC, in relation to the physical member. A node joins a strong group, which is unicast with its own KEK. The other KEKs nodes must be updated by multiplying a GKC message containing the new KEKs (all of them O(log2n) for a balanced tree). Each substitution KEK is encoded twice by the KEK of each of its children, resulting in an entire message sized 2log2n. A comparable algorithm is used to maintain future protections for leaving members. In [11], there is also an inquiry into a logical key hierarchy, considering the fact that a hybrid structure with an Iolus-like physical hierarchy will map such network topologies.

The One-way Function Tree (OFT) [12] algorithm uses the same topology as LKH but also increases the message size to O(log2n), primarily by generating a KEK set based on one set of children's keys after executing a one-way element. In addition, the OFT method is restructured to produce OFT+. In the other hand, a hash function is only functional to the community key in OFT+ other than LKH+ in which a hash function is applied on all the affected keys.

Efficient Broad Community Key Distribution (ELK) [13] also uses a simulated hierarchical key and OFT-like rebuild method to generate a pseudo-random function (PRF) key from a member's node. ELK uses 'hint' to count UDP multicast reliability. A 'hint' is a partial key that can be produced by the test and error process. As a part of a key can not be established, protection is not affected.

6. PROPOSED EFFICIENT GROUP KEY MANAGEMENT SYSTEM

The region-based Key Management Protocol divides a population into regions-based subgroups, based on the decentralised key management principles using a Weighted Clustering Algorithm (WCA). A SERGK for MANETs is suggested in this approach. The fundamental concept of SERGK is to form an efficiency physical multicast tree in MANETs. Group members receive turns to carry out intermediary primary materials for group members and exchange them with them. The main materials are scattered over the ties of the tree. The supervisor is also responsible for managing the multicast community connection. All group members can locally measure the group key in a distributed way.

SERGK scheme is presented as follows:

i. Notations and Assumptions

It is assumed that a legitimate certificate from offline arrangement is performed by each node prior to entering the network. A smart card can be used for this pre-configuration. As a result, there is a fundamental public key infrastructure to manage certificates. When referring to the literature, most solutions suffer the man-in-the-middle attack.

Table 1 : 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, =
k_i	Internal node i's key, $k_1=(bri)^{ki}$, also called intermediate key
bk_i	Blinded internal node i's key, $B_{ki} = g^{ki}$, also called blinded intermediate key
$h(m)$	The digest of
K_G	The common group key

In this proposed approach, it is implicit that each group member has a distinctive identifier and all keying materials are digitally signed by related initiators to guarantee 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 take some secret information (for instance, password) with the purpose of joining the group or a node can join a group if it can provide 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 Table 1.

ii. Key Management by SERGK Approach

Every group member contributes a share of the ultimate common group key, to structure 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 updation of the group key assists to impose 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. An indigenous broadcast through flooding is clearly not suitable as a result of large redundancy which may possibly result in network traffic congestion. Here, a consistent double multicast tree formation and protection protocol is presented. This scheme is similar to Wei and Zakhor [14], on the other hand, the double tree scheme ensures that two trees cover all group members. Logically, the two trees are the same from a group member's approach. In this double tree scheme, some group members incorporated in one tree might not be incorporated in the other tree, which is clearly not desirable for GKM. The multicast routing protocol works as a subsystem of the GKM framework.

Group initialization process is started by a group initiator by transmitting a join advertise message across the complete network. A sequence number is used to avoid loops. A node is coupled with three colors, namely blue, red and grey. A node will select grey as its color when sum of its neighbor is less than a predefined threshold value (for instance, half of average node degree). All member nodes are grey. Other network nodes choose a random blue or red colour with an odds of 0.5. A grey node saves the upstream node ID and retransmits the message for the first message received.

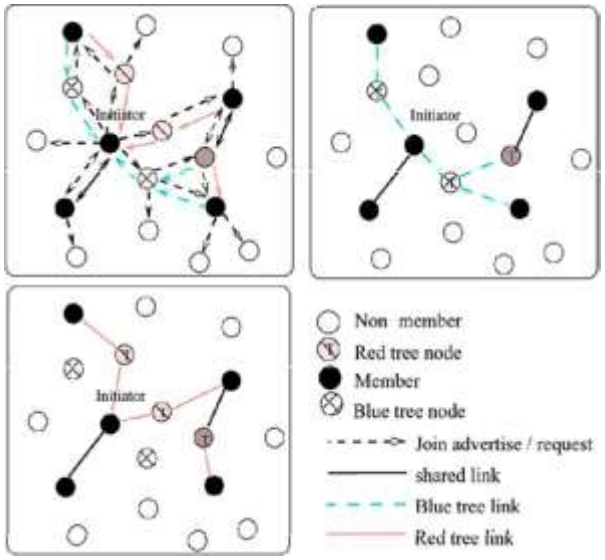

Figure 1: Illustration of a double multicast tree structure

For a non-gray node, the upstream node is accumulated and retransmitted only if the upstream node is identical in colour, sender, or grey node. In parallel, multiple double multicast trees are generated based on the response of a group member to the group initiator. Both trees are group members and non-member intermediary nodes. A node could submit requests for membership to a community. Any current member of the community will return responses. The method of handling demands for membership is equivalent to community ads to ensure the durability of double multi-cast tree systems. The resulting two trees can be separated or a single node. A complex double multicast tree structure is developed. Figure 1 demonstrates how a double multicast tree is created.

iii. Construction of Double Multicast Trees

The approach above met a challenge, namely that the two multicast trees may not be the same, suggesting that certain classes of members may be protected by a blue tree but are not merged into the red tree. This situation is possible if a member of the party is connected by nodes of just one colour, red or blue. This can be observed by a community member if messages have only been sent in one colour (whether blue or red) of the nodes. This node will then need one of its upstream nodes to convert colour into grey.

Initially, the community initiator takes care to send out refresh messages constantly to keep the double multi-cast tree system linked. A group member might decide to serve as group organiser after a certain period of operating time and notify the group that he is obligated to retain the group. Both members must serve as community coordinators. Double multicast trees are available for use, allowing one tree to be active and the other tree to be stored in a stationary state. The multicast trees were created after a certain period of time for the group initialization process, and the group coordinator could follow the group key development method. This technique is outlined in detail in the main community.

iv. Detection of Leaving Members

The Member's departure is more difficult to handle than the joining of new members. A new user is expected to submit a request to access the party. Once an established group member or the existing group coordinator approves his application, the new user becomes an approved group member. However, it cannot be concluded that a departing member sends a departure message for the situation of leaving members. Without any information a member could leave the group. Even if a message could be received and informed, this message could be lost in a complex world. A physical exit and a logical exit may be described. A node pushes beyond the control of the network or turns off its transmitter for the physical escape. In order to exit logically, a node stays in the network, but does not partake in group operation.

Two methods are presented to address these problems

a. First Method

The first technique of the method is that the new GC constantly sends refresh messages to members via all tree connections. All community members must give an ACK message to their association interests (status). The community coordinator shall decide whether a member stays attached or leaves within a certain period of time in line with the reply. It is the member's responsibility to retransmit a message to the community under a restricted flood scheme if the periodic member does not hear a refreshing message. If a member does not wish to be a party member, they will stay silent until the ACK message is received. The structure of the tree is updated with the control messages. Any connections can be truncated and new links can be inserted as a member can switch to a new position. The established GC notifies all participants of the change event through the revised tree structure. This technique is highly successful and ideal for a reasonably static network environment.

b. Second Method

The second method has another strategy that the group initiator or current group coordinator periodically broadcasts member enforcement messages in a controlled flooding scheme. The predetermined flooding range is fixed to the maximum distance from the coordinator to the members. The search range can be enlarged until it reaches a threshold value or the current network diameter. All group members will transmit a

response back. As a result, members associated with the group are refreshed. This strategy is quite costly compared with Method one and is more suitable for extremely dynamic setting in which nodes move frequently and cause the connections to be broken frequently.

i. Group Key Establishment Protocol

The fundamental concept of a group key agreement protocol is that all group members preserve a logic key tree in local storage space. The key tree is exploited to work out the final common group secret. Several contributing group key approaches maintain a certain kind of key repository. But they show certain difference in the manner they store and distribute intermediary 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. Even though the proposed key tree is identical to STR, several improvements are introduced as describe below. The key tree structure in SERGK is shown in Figure 2.

- To share the workload of keying service, the idea of coordinator is introduced. The coordinator is accountable for computing and distributing intermediary keys to all group members which take part in communication. It is also necessary to manage member join and leave. The responsibility of coordinator revolves around all members.

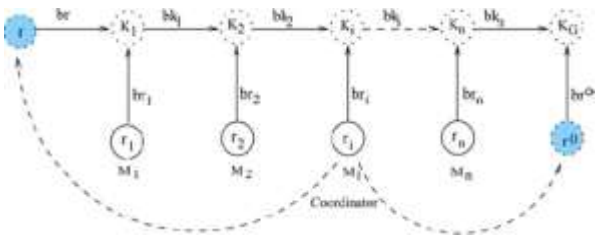

Figure 2: Illustration of Key Tree Structure

- 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 GC role switching.

- A new group member can be effortlessly immersed into the group by incorporating new members into the current rightmost position and moving itself to the right.

- When a member leave is detected, the coordinator produces a new random key ‘r ’ and multicast the blinded value br in addition to other intermediary blinded keys.

► *Group Key Initialization*

The coordinator declares its responsibility and broadcasts two arbitrary keys ‘r’ and r_0, at the initialization stage. In general, 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. On the other hand, at following member add events, a new member is constantly 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 completed perfectly by the coordinator because it requires to multicast blinded intermediary keying materials to all group members. All keying materials are placed in one package and the order of blinded intermediary key materials shows the structure of the key tree.

Group Key Initialization Algorithm:

1. Round 1: The group initiator, Mc, *i* ∈ [1, n] advertises a blinded random member key br_c and two virtual blinded member keys br and br_o. Each interested member M, *i*, ∈ [1, n], i ≠ c responds with a blinded random member key.

2. Round 2: The initiator M_c computes intermediate keys $k_i = (br_i)^{ki-1}$ and multicasts blinded intermediate keys $bk_i = g^{ki}$, ∀i ∈ [1, n]. $K_0 = r$.

3. Every M_i, I ∈ computes $k_i = (bk_{i-1}^{r_j})(k_0 = r)$ and recursively $k_j = (br_j)^{k_{j-1}}, \forall j \in [i, n], K_G = br_n^{k_n}$.

► *Member Addition*

A new group member can be added without any difficulty into the group by introducing it into the existing rightmost position and moving the dummy coordinator to the right. The most important improvement of this approach is that the coordinator does not need to produce a new arbitrary key but still provides key independence. This means that knowing the previous group key cannot help to deduce the new group key. Two blinded keys are provided, the new member can work out the new group key and on the other hand, it cannot work out the former group key. This guarantees backward secrecy. Figure 3 illustrates the operation of joining a new member.

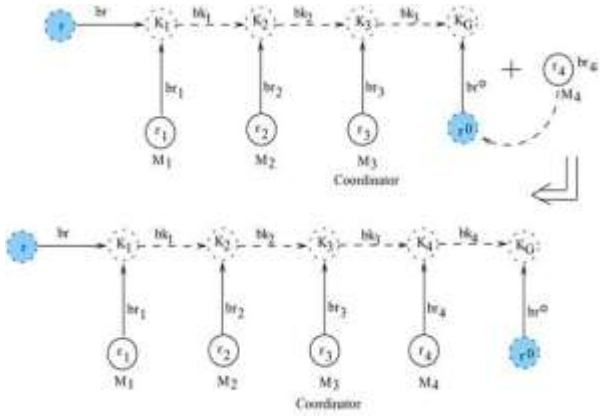

Figure 3: Illustration of Key Updating for Joining Member

Member Addition Algorithm:

1. Round 1: New member M_{n+1} generates a random member key r_{n+1} and broadcasts the blinded value br_{n+1}. The coordinator unicasts the blinded keys bk_n and b_{ro} to the new member.

2. Every $M_i, i \in [1,n]$ computes $k_{n+1} = (br_{n+1})^{k_n}$ the new member computes $k_{n+1} = (bk_n)^{r_{n+1}}$ and $M_i, i \in [1,n+1]$ can compute $K_G = br_o^{k_{n+1}}$

► *Member Leave*

The leaving group member event can be identified either by clear notification from the leaving node or through the scheme described before through Method one or Method two. The coordinator informs all group members of the member leaving event and multicasts a new blinded arbitrary key to all members.

The new group key can be computed by all group members. Figure 4 demonstrates the working of a departing member.

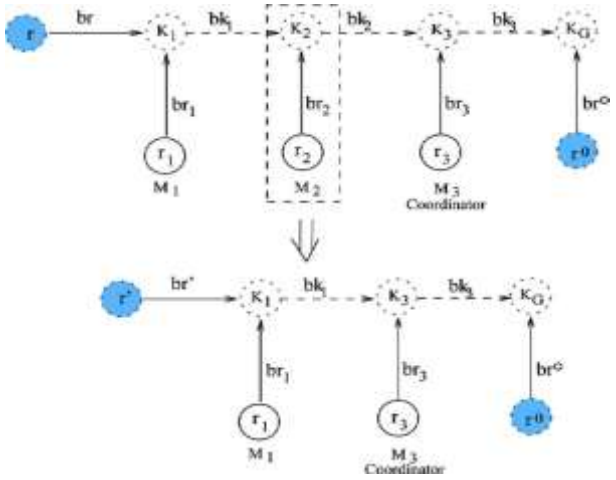

Figure 4: Illustration of Key Updating for Leaving Member

Member Leave Algorithm:

6. CONCLUSION

Key ad-hoc network management is a complicated matter with respect to community contact stability. This chapter offers an introduction to the creation and study of core regional management protocols for MANETs with flexible and reconfigurable community key management. The suggested simple, effective group key management protocol divide an organisation by the Simple Efficient Region-based Key Management Protocol (SERGK) into region-based subgroups based on decentralized main management concepts. There is a group member operating as a group coordinator in this method, who computes and distributes the Group's blinded intermediate keying information. Each participant calculates the community key spread. The position of community coordinator shall be rotated among all participants to disperse the workload of group rekeying and maintenance. A new main tree structure is implemented to efficiently modify the group control function.

7. REFERENCES

1. Renu Dalal, Yudhvir Singh and Manju Khari (2012). A Review on Key Management Schemes in MANET, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, DOI : 10.5121/ijdps.2012.3417, pp. 165- 172.

2. El-Sayed A. (2013) Clustering Based Group Key Management for MANET. In: Awad A.I., Hassanien A.E., Baba K. (eds) Advances in Security of Information and Communication Networks. SecNet 2013. Communications in Computer and Information Science, vol 381. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40597-6_2

3. Qiuna Niu (2014). "ECDH-based Scalable Distributed Key Management Scheme for Secure Group Communication," Journal of Computers vol. 9, no. 1, pp. 153-160.

4. Priyanka Ahlawat (2019). International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-2S, December 2019.

5. Ayman EL-SAYED, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 4, 2014. A new Hierarchical Group Key Management

based on Clustering Scheme for Mobile Ad Hoc Networks.

6. Atul Adya, Paramvir Bahl, Jitendra Padhye, Alec Wolman and Lidong Zhou (2004). “A Multi-radio Unification Protocol for IEEE 802.11 Wireless Networks”, International Conference on Broadband Networks, pp. 344- 354.

7. Paul Judge and Mostafa Ammar (2003). “Security Issues and Solutions in Multicast Content Distribution: A Survey”, IEEE Network, pp. 30-36.

8. Harney H, Muckenhirn C and Rivers T. (1994). “Group Key Management Protocol Specification”, RFC 2093.

9. Hardjono T and Dondeti L R (2003). “Multicast and Group Security”, Artech House, Boston, MA.

10. Wittman R. and Zitterbart M. (2002). “Multicast Communication – Protocols, Programming and Applications”, Morgan Kauffman, San Francisco, CA.

11. Wong C. K., Gouda M. and Lam S. S. (2000). “Secure Group Communication using Key Graphs”, IEEE/ACM Transactions on Networking, Vol. 8, No. 1, Pp. 16-30.

12. McGrew D. and Sherman A. (2003). “Key Establishment for Large Dynamic Groups using One Way Function Trees”, IEEE Transactions on Software Engineering, Vol. 29, No. 5, pp. 444-458, 2003.

13. Perrig A., Song D. and Tygar J. D. (2001). “ELK: A New Protocol for Efficient Large-Group Key Distribution”, IEEE Security and Privacy Symposium, pp. 247-262.

14. Wei Wei and Avideh Zakhor (2004). “Robust Multipath Source Routing Protocol (RMPSR) for Video Communication Over Wireless Ad Hoc Networks”, International Conference on Multimedia Computing and Systems/International Conference on Multimedia and Expo, Pp. 1379-1382.

Corresponding Author

Tilak Singh Rajput*

Research Scholar, Department of Computer Science, Sri Satya Sai University of Technology & Medical Sciences, Sehore, M.P.