A Novel Rekeying Function Protocol based on Region based Group Key Management

Dr. N. Vimala, Assistant Professor, PG Department of Computer Science, LRG Govt. Arts College for Women, Tirupur.

Dr. K. Saraswathi, Assistant Professor, PG and Research Department of Computer Science, Govt. Arts College, Coimbatore.

Abstract

In wireless networks, most of the centralized key management protocols are having the security issues in a data communication. This arises some cryptography key management protocols to be proposed to taken care on the issues and in securing the data. Here the region-based group key management protocol is proposed and divides a group into region-based subgroups based on decentralized key management principles using Novel Rekeying Function Protocol (NRFP). This improves scalability and efficiency of the key management approach in providing group communication in a secure manner.

Keywords: *Data Security, Key Management Protocol, Scalability.*

I. INTRODUCTION

Wireless network is a kind of computer network that is wireless and is generally connected with a telecommunications network and the interconnections between nodes are connected without using any wires. The realization of wireless telecommunications networks would be with certain kind of remote information communication system that utilizes electromagnetic waves, like radio waves, for the carrier of information and this way of implementation generally takes place at the physical level or layer of the network[1].

The revolution in the field of wireless communication [2] is bringing essential transformation to data networking, telecommunication and making integrated networks a reality. Ad-hoc networks are widely used in the field of networking.

Ad-Hoc Networks

The Latin meaning of the word ad-hoc is “for this purpose”. It significantly points out that network generated for a particular purpose. In general, these networks consist of a collection of workstations or additional wireless devices which communicate directly with each devices or workstations in order to interchange information.

Ad-hoc network is a kind of network in which there are no access points interchanging information between the different participants. The information of the infrastructure networks normally pass through a middle information hub which would be a hardware device or software on a computer. Organization networks commonly use a server to which company workstations attach with the purpose of collecting the information. However, in this case the networks do not pass through a middle information hub.

Ad-hoc networks are generally closed, because it is not attached to the internet and are generally formed between participants. However, when one of the participants initiates a connection to a public or private network, this connection can be common between other participants of the ad-hoc network. This process permits additional users on the spontaneous ad-hoc network to connect the internet additionally.

Working of Wireless Multicast:

Wireless multicasting route using different approaches: In the tree-based technique, multicasting utilizes a shared tree. Only one path exists between any pair of nodes. Core-based multicast can also be used. But, if node failure happens then the entire tree is likely to be interrupted. This technique is mainly utilized in ad-hoc wireless networks that offer a high degree of mobility for all network components.Multicast routing which makes use of a mesh needs more resources than a tree. A mesh is generated to set up connectivity and facilitates multiple paths between a pair of nodes.

Topology-independent routing, which transmits packets in various directions without using a formal routing structure.Fixed-topology multicast routing aids some protocols such as the Distance Vector Multicast Routing Protocol (DVMRP), Multicast extension to Open Shortest Path First (MOSPF), and Protocol Independent Multicast (PIM). This is appropriate for infrastructure-based wireless networks.The following factors are very essential while providing multicast services in wireless environments [3] battery power, bandwidth constraints, host mobility, loss of packets, and wireless security issues

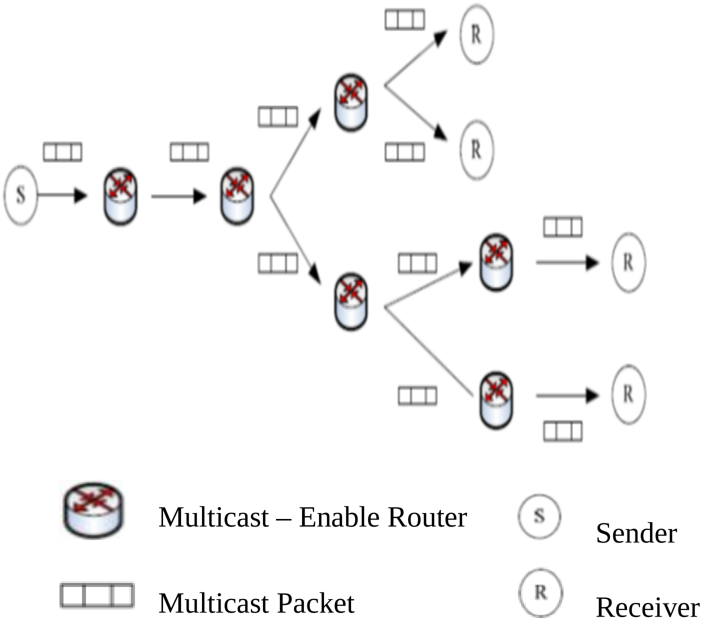

Figure 1: Multicast Transmission Mechanism

The rest of this paper is organized as follows: Section II review of Literature survey onkey management protocols merits and demerits. Section III discusses on proposed methodology. Section IV Results and Discussions tell about the achieved results and discussed the overcome demerits of the existing system. Section V concludes with conclusion and future developments.

II. LITERATURE SURVEY

Maghmoumi et al., in [4] proposed a cluster based scalable key management protocol for Ad-hoc networks. This protocol was based on a new clustering technique. The network was partitioned into communities or clusters based on affinity relationships between nodes. In order to ensure trusted communications between nodes proposed two types of keys generated by each cluster head. The protocol is adaptive according to the limitation of the mobile nodes battery power and to the dynamic network topology changes. Their proposed approach of clustering based scalable key management protocol provided secured communications between the nodes of the Ad-hoc networks.

A key management scheme for secure group communication in MANETs was described by Wang et al., in [5]. A hierarchical key management scheme (HKMS) was described for secure group communications in MANETs. For the sake of security, a packet was encrypted for two times. The author also discussed group maintenance in order to deal with changes in the topology of a MANET. Finally, the author carried out a performance analysis to compare this scheme with other conventional methods that are used for key management in MANETs. The results showed that this method performed well in providing secure group communication in MANETs.

George et al., [6] projected a framework for key management that provides redundancy and robustness for SA establishment between pairs of nodes in MANETs. In this framework a modified hierarchical trust Public Key Infrastructure (PKI) model was used in which nodes can dynamically assume management roles. Moreover, the author employed non-repudiation through a series of transactions checks to securely communicate new nodes information among CAs. The author assumed that nodes could leave and join the network at any time. Nodes could generate their own cryptographic keys and were capable of securing communication with other nodes. In order to balance 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 sustained sufficient levels of security by combining node authentication with an additional element, node behavior. A behavior grading scheme required each node to grade the behavior of other nodes.

A new GKM protocol for wireless ad-hoc networks was put forth by Rony et al.,[7]. They put forth an efficient group key distribution (most commonly known as group key agreement) protocol which is based on multi-party DH group key exchange and which is also password-authenticated. The fundamental 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 proposed protocol starts by constructing a spanning tree on-the-fly involving all the valid nodes in the scenario. It is understood, like all other protocols that each node is distinctively addressed and knows all its neighbors. The password 'P' is also shared among each valid member present in the scenario. This 'P' helps in the authentication process and prevents man-in-the-middle attack. Unlike many other protocols, the proposed approach does not need broadcast/multicast capability.

Bechler et al., [8] presented cluster-based security architecture for Ad-hoc networks. The author proposed and computed a security scheme depending on a distributed certification facility. A network is partitioned into clusters with one special head node for each cluster. These cluster head nodes carry out administrative operations and shares a network key among other members of the cluster. Furthermore, the same key is utilized for certification. In each cluster, exactly one differentiated node called the Cluster Head (CH) is accountable for developing and organizing the cluster. Clustering is also employed in certain routing protocols for ad-hoc networks. Decentralization is attained via threshold cryptography and a network secret that is distributed over a number of nodes. The architecture deals with the issues of authorization and access control and a multi-level security model aids to regulate the complexity to the abilities of mobile end systems. Depending upon their authentication infrastructure, the author offered a multi level security model assuring authentication, integrity and confidentiality.

A scalable key management and clustering approach was presented by Jason et al., [9]. The author proposed a scalable key management and clustering approach for secure group communications in ad-hoc networks. The scalability issue is handled by dividing the communicating devices into subgroups, with a leader in each subgroup and further organizing the subgroups into hierarchies. Each level of the hierarchy is known as a tier or layer. Key generation, distribution and actual data communication follow the hierarchy. Distributed Efficient Clustering Approach (DECA) offers significant clustering to produce subgroups and it is observed from the simulation results that DECA is very efficient in terms of energy and resilient against node mobility. When compared with other existing approaches, DECA technique is extremely scalable and significant and ensures high security.

Laurent Eschenauer et al., [10] presented a key management approach that guarantees the authenticity of distributed network. Distributed Sensor Networks (DSNs) are Ad-hoc mobile networks that comprise sensor nodes with restricted computation and communication abilities. The functional and security necessities of DSNs can be fulfilled by a key management approach presented by the author. Furthermore, the approach also consists of selective distribution and revocation of keys to sensor nodes as well as node re-keying without considerable computation and communication abilities.

Ricardo StaciariniPuttini et al., [11] described a novel authentication service for securing MANET routing protocols. An authentication service is regarded as a fundamental defensive protection for the routing protocol.

A novel efficient Hierarchical Binary Tree (HBT) Model to form Ad-hoc group was presented by Erdem [12]. This system uses a new key distribution approach to bring an unfamiliar device to group and to exchange a secret key at that moment. The binary tree model proposed is an Efficient Distributed Key Management (EDKM) model. The main properties that are considered in EDKM are self-organizing and can be employed incrementally in the network. When EDKM is compared with other HBT technique, it is presented that EDKM offers whole backward and forward security in case of modification in the membership and furthermore it does not enhanced the processing or storage necessities. The model presented is based on the one-way hash function and the secret key cryptography. Therefore, EDKM seems to be very effective and practical for MANETs.

A Security approach was proposed by SugataSanyal et al., [13], for distributed DoS in MANETs. Due to intrinsic drawbacks of the routing protocols used in MANETs several types of DoS attacks are possible on MANET. The author proposed a proactive approach that can avoid a particular type of DoS attack and discover the misbehaving node. The performance of approach in a series of simulations showed that the proposed approach offers a much better solution than the conventional techniques with no extra overhead. The proposed technique shifts the responsibility to monitor the parameters of the compromised node on the node's neighbor, thus assuring the compliance of restriction. This eradicates the issues because of flooding of Route REQuests (RREQs) from the compromised node.

Aldar Chan and Edward Rogers [14] proposed a distributed symmetric key management for MANETs. Conventional key management techniques are too inefficient, not functional on an arbitrary network or unknown network topology, or not tolerant to a changing network topology or link failures. Therefore, it is not appropriate for Ad-hoc networks. Key Pre-distribution Schemes (KPS) are the only suitable option for cases where the network topology is not known previous to deployment. However, this approach depends on TTP. The technique presents Distributed Key Pre-distribution Scheme (DKPS) and generates the first DKPS prototype to realize fully distributed and self organized key pre-distribution without depending on any infrastructure support. This technique of implementing DKPS avoids the limitations of the traditional techniques.

A novel approach to ensure the security of MANETs was proposed by Fagen Li et al., [15]. The author presented a distributed key management technique by exploiting the self-certified public key system and threshold secret sharing approaches. The use of self-certified public key system in this technique had the advantages such as reduction in the storage space and the communication overheads. Moreover, the computational costs can be reduced as it needs no public key verification. The key escrow issue is also eliminated as the CA does not know the user's private keys. This technique is much better and efficient when comparing it with the certificate-based public key system and IDentity-based (ID-based) public key system. Table 1 summarizes the comparison of various algorithms discussed on literature based on five major security services of MANET.

Table 1: KEY FEATURES OF MANETs ROUTING PROTOCOL AND MAE REQUIREMENTS FOR EACH PROTOCOL
DS is the Digital Signature and HC denote Hash Chain

Routing Protocol	Routing Discovery	Routing Algorithm	Relevant Message	Authorized objects
DSR	On-Demand	Source routing	RREQ	DS+HC
			RREP	DS
AODV	On-Demand	Distance vector	RREQ	DS+HC
			RREP	DS+HC
			RERR	DS
			RREP-ACK	DS
OLSR	Proactive	Link state	Hello, TC	DS
TBRPF	Proactive	Link state	Hello, TU	DS

In Table 1, DSR represents Dynamic Source Routing protocol, AODV is Ad-hoc On-demand Distance Vector routing protocol, OLSR is Optimized Link State Routing protocol, and TBRPF is Topology dissemination Based on Reverse-Path Forwarding protocol. In the similar way RREQ represent Route Request, RREP denote Route Reply and RRER stand for Route Error, TC represents Topology Control and TU denotes Topology Update.

III. PROPOSED METHODOLOGY

Most of the centralized key management protocols arises an issue on data security on group communication. The proposed Novel Re-keying Function Protocol (NRFP) divides a group into region-based subgroups based on decentralized key management principles. The partitioning of region into subgroups improves scalability and efficiency of the key management approach in providing group communication in a secure manner.

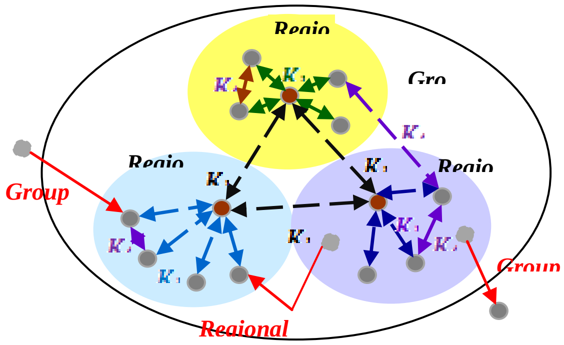

Figure 2: Region-based Group Key Management

Figure 2 shows the partitioning of region into subgroups on the basis of decentralized key management principles [16, 17]. It is assumed that each member of the group is equipped with Global Positioning System (GPS) and therefore each one knows its location as it moves across the regions. For secure group communications, all members of a group share a secret group key, K_G. In addition to ensure 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}. shared secret key is constructed and controlled by a distributed group key management protocol that enhances robustness. This NRFP will function at the optimal regional size recognized to reduce the cost of key management in terms of network traffic.

Instead using conventional encryption algorithms, the proposed scheme employs an MDS code which is a class of error control codes, to distribute multicast key dynamically. This scheme considerably reduces the computation load of each group member compared to existing schemes employing traditional encryption algorithms. Such a scheme is advantageous for many wireless applications where portable devices or sensors need to reduce their computation as much as possible because of battery power limitations. Simply combined with any key-tree-based schemes, this scheme affords much lower computation complexity while maintaining low and balanced communication complexity and storage complexity for secure dynamic multicast key distribution.

The nodes must contain the following keys: Master Key (MK), is shared by all the nodes in the network; Local Key (LK), is shared with the Base Station (BS); and the Session Key (SK), is shared with other nodes which take part in the communication. Each of these keys is taken into consideration which in turn with the reasons for incorporating it in the prototype.

For a MAC function, a MAC algorithm can be produced using several different approaches, as long as the sender and receiver have shared secret keys. A MAC algorithm can be created from a common symmetric cipher.

IV. RESULTS

The simulation was implemented in NS-2. 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[18] with the existing RGK[19] 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. Table 2 and Figure 4 shows the average computation cost of the different rekeying protocols along with the proposed approach.

Number of Nodes	Average Computation Cost (p=10%)		
	RGK	SERGK	NRFP
60	250	115	90
80	410	240	120
100	510	320	185

120	640	450	210
140	840	510	255
160	1500	660	315
180	1800	820	370
200	2300	990	400

Table 2: AVERAGE COMPUTATION COST OF THE PROPOSED APPROACHES

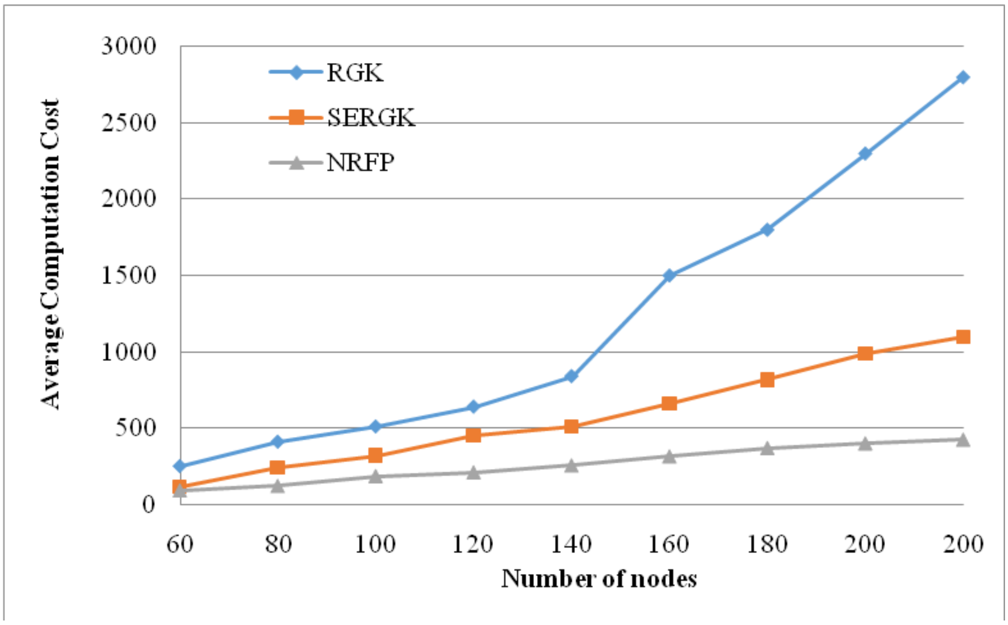

Figure 4: Comparison of Average computation time for the proposed approaches

V. CONCLUSION

This research focuses on the establishment of the effective key management for MANETs with the use of group key management. Novel Rekeying Function Protocol with Multicast Key Distribution provides more security and reliability with better computation time and cost, member join and leave, group communication cost and delivery ratio. To improve the performance of the proposed technique, certain future enhancement is necessary for this research work which would be based on the following, i) Key management techniques can be used with the secret sharing scheme for better security and ii) Research can be done on hashing functions and novel hash functions can be utilized to reduce the communication overhead.

REFERENCES

[1] Atul Adya, ParamvirBahl, JitendraPadhye, Alec Wolman and Lidong Zhou "A Multi-radio Unification Protocol for IEEE 802.11 Wireless Networks", International Conference on Broadband Networks, Pp. 344-354, 2004.

[2] Saad E M, El Adawy M, Keshk H A and Shahira M Habashy, "Reconfigurable Parallel Processor System based on Ant Colony Algorithm", Proceedings of the Twenty Third National Radio Science Conference (NRSC), Pp. 1 – 11, 2006.

[3] Vasudevan V and Sukumar R, "Enhancing the Scalability of Secure Wireless Multicast", Journal of Computers, Vol. 20, No. 3, Pp. 47-54, 2009.

[4] ChadiMaghmoumi, HafidAbouaissa, JaafarGaber 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.

[5] 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.

[6] 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.

[7] 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.

[8] Bechler M, Hof H J, Kraft D, Pählke F and Wolf L, "A Cluster-based Security Architecture for Ad Hoc Networks", 23rd Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 4, Pp. 2393-2403, 2004.

[9] Jason H Li, Renato Levy, Miao Yu and Bobby Bhattacharjee, "A Scalable Key Management and Clustering Scheme for Wireless Ad Hoc and Sensor Networks", Future Generation Computer Systems, Vol. 24, No. 8, Pp. 860-869, 2008.

[10] Laurent Eschenauer and Virgil D Gligor, "A Key Management Scheme for Distributed Sensor Networks", Proceedings of Ninth ACM Conference on Computer and Communications Security, Pp. 41-47, 2002.

[11] Ricardo StaciariniPuttini, Ludovic Me and Rafael Timoteo de Sousa, "Certification and Authentication Services for Securing MANET Routing Protocols", Proceedings of fifth IFIP-TC 6 International Conference, Pp. 278-281, 2003.

[12] Erdem O M, "EDKM: Efficient Distributed Key Management for Mobile Ad Hoc Networks", Proceedings of 9th IEEE Symposium on Computers and Communication, Vol. 1, Pp. 325-330, 2004.

[13] SugataSanyal, Ajith Abraham, DhavalGada, RajatGogri, PunitRathod, ZalakDedhia and NiraliMody, "Security Scheme for Distributed DoS in Mobile Ad Hoc Networks", International Workshop on Distributed Computing, Pp. 541-542, 2004.

[14] Aldar C F Chan and Edward S Rogers, "Distributed Symmetric Key Management for Mobile Ad Hoc Networks", Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), Vol. 4, Pp. 2414 – 2424, 2004.

[15] Fagen Li, XiangjunXin and Yupu Hu, "Key Management in Ad hoc Networks using Self-Certified Public Key System", International Journal of Mobile Communication, Vol. 5, No. 1, Pp. 94-106, 2007.

[16] Chatterjee M, Das S K and Turgut D, "An On-Demand Weighted Clustering Algorithm (WCA) for Ad hoc Networks", Proceedings of IEEE Globecom'00, Pp. 1697–1701, 2000.

[17] 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, 2008.

[18] N.Vimala and Dr. R. Balasubramanian, A New Region Based Group Key Management Protocol for MANETs, International Journal of Computer Science and Information Security, Vol. 8, No. 2, Pp. 194-200, May 2010.

[19] N.Vimala and Dr. R. Balasubramanian, Efficient Group Key Management Protocol for Region Based MANETs, International Journal of Engineering And Technology, Vol. 3, No.1, Pp. 68-75, February 2011.