International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 3 (September '2017)
Proceeding of - International Conference on Recent Trends in Computational Life Science and Information Technology,
Conference held at Tiruppur Kumaran College for Women,Tirupur,Tamilnadu, India.

EFFICIENT GROUP KEY MANAGEMENT PROTOCOL FOR DDOS ATTACKS

Dr.C.Kalaiselvi,
Associate professor and Head,
Department of Computer Applications,
Tiruppur Kumaran College for women,
Tiruppur,Tamilnadu,India.

G.Arunasenbagam,
M.Phil., Research Scholar,
Department of Computer Science,
Tiruppur kumaran College for women,
Tiruppur,Tamilnadu, India.

Abstract: Key management in the unprepared network is an exigent problem concerning the security of the group communication. There are three categories for classifying Group key management protocols; centralized, decentralized with distributed. in establishing key management *protocol*, suitable solution can be provide to services like verification, data reliability and data confidentiality. This paper deals by an approach for designing and analyzing the region-based Group key management protocols in support of scalable and reconfigurable group key management in Mobile unprepared Networks (MANETs). The main problem of centralized key management protocols is a propos data security planned group communication. To rise above this problem a narrative approach for key management into Region based MANET is proposed. The Group key organization comprises creating and distributing a common covert for all the group members. However, key management for a large and dynamic group be a difficult problem because of scalability and security. adjustment of membership requirements the group key to be refreshed to make sure backward and forward secrecy. In this paper, a Robust and Efficient Group Key(REGK) management scheme be proposed for Region based MANETs. The proposed method is as well effective in defending against many complicated attacks such as rejection of service (DoS) attack. In order toward preserve the security, the region-based group key management protocols deal with stranger attacks in MANETs. The experimental results compares the calculation cost moreover time for the existing and proposed approach and the results illustrate so as to the proposed approach outperforms the existing method through lesser calculation cost and time.

Keywords : Cluster Head, Group Key, Key Management Protocol, Mobile Ad Hoc Networks (MANETs), Region-based and Rekying

I.INTRODUCTION

Basically, an unprepared network is a collection of independent nodes which communicate with each other, the majority obviously through using a multi-hop wireless network. Nodes do not predictably identify each other and come mutually to form an unprepared network, only on behalf of some particular reason. Key distribution systems perform as a trusted third party (TTP) to proceed as an intermediary connecting nodes of the network. A node has straight connection by way of a set of nodes, said to exist neighboring nodes, in an unprepared network which be in its communication range. The number of nodes in the network is not basic preset. at any time the new nodes connect the network, the older nodes be considered to exist un-functional [1]. Key management within the unprepared network be a main drawback, in terms of security of the group communication. The three categories used for Group key management protocols be; centralized, decentralized, and distributed [2].

MANET has no programmed infrastructure such the same as base stations otherwise mobile switching centers (MSC). Wireless network plays a vital role within terms of communication; Mobile nodes be able to exist communicated directly by means of a wireless network through radio waves, anywhere because those far apart rely on other nodes to act as routers toward relay its messages [3]. The nearly everyone suitable solution toward provide the services among which authentication, data integrity in addition to data confidentiality is the establishment of a key management protocol. Traffic encryption key (TEK) be used for generation along with distribution of each and every one the members in a group. This key is mainly favored through the source to encrypt multicast data and the receivers to decrypt it. so legal members be able to only receive the multicast flow which is sent by the group source and additional members are not allowed toward receive the flow [4]. The key synchronism, secrecy, freshness, independence, authentication, and confirmation,

Forward plus backward secrecy are the elemental security services provided by each key management system [7].

Cluster is eventually assumed to be group, while clustering is a occurrence of collecting sub groups. Local controller (LC) is used to manage all sub-group, liable for local key management surrounded by its own cluster. Energy constitutes a leading concern in unprepared environments, moreover, not many solutions for multicast group clustering do think about the energy problem to realize an efficient key distribution process [5] [6]. Cluster beginning generates group key which communicate to other members from side to side a secure and constrained channel with the purpose of uses public key cryptography [14]. Clusters can be used for achieving different targets [8]. Clustering for transmission management, back formation, and for routing efficiency are several of ways for achieving different target. By outsiders

plus rouge members, group key management can live opposed to a broad range of attacks.

II.BACKGROUND STUDY

A Key management is a dynamic part of any secure communication. Most cryptosystems rely on some essential secure, robust, and efficient key management system. This division 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 separated into communities or clusters based on affinity relationships between nodes. A key management proposal for secure group communication in MANETs was described by Wang et al. in [10. The results demonstrate that their proposed method performed well in providing secure group communication in MANETs.

George et al. in [11] 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 linking node authentication with an additional element, node behavior.

A original group key management protocol for wireless communication ad hoc networks was stated by Rony et al. in [12]. 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 well-known 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 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

III.PROPOSEDMETHODOLOGY

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.

Protocol Description

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

- **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.

- **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.

- **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 (REGK) scheme is presented as follows

- **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.

- **Key Management by REGK 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 REGK, 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.

- **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.

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 keymanagement 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 REGK 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.

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. In this paper that 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 (REGK)

VI. 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.

[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

[19]. networks', International Workshop on Wireless Ad Hoc Networks (IWWAN 2004), Oulu, Finland, pp.270– 274.