International Journal of Future Generation Communication and Networking
Vol. 9, No. 11 (2016), pp. 345-352
http://dx.doi.org/10.14257/ijfgcn.2016.9.11.32

Survey of Group Key Management Techniques in MANET

G.Narayana[1*], M.Akkalakshmi [2] ,A.Damodaram[3]

[1]*Associate Professor,Dept of CSE,Joginpally B.R Engg.College,Hyderabad,Telangana, India*
[2]*Professor, Dept of IT, GITAMS Uiversity,Hyderabad, Telangana,India*
[3]*Vice-Chancellor, Sri Venkateswara University, Tirupati, Andhrapradesh, India*
**Email:narayangphd@gmail.com*

Abstract

Group key management (GKM) technique is employed for ensuring security and integrity in Mobile Ad hoc Networks (MANET). It is the fundamental component of secure group communication systems. It involves distribution, updation and revocation of group keys. GKM can be carried out through many approaches. Existing studies on GKM techniques in MANET did not provide detailed analysis. This survey presents various GKM techniques for MANETs. The existing GKM techniques are classified into three categories namely centralized, distributed and hierarchical. Each of these techniques are explained with their advantages and disadvantages.

Keywords: *MANET; Key Management; AODV; Security; Authentication; CRT*

1. Introduction

Currently, mobile ad hoc networks (MANETs) are deployed in several areas ranging from military, emergency, and rescue mission to other collaborative applications for commercial use. The security concerns of such network are heightened by the rapidly growing application of MANETs. Secure and efficient group key agreement protocols have gained a lot of attraction in MANETs. A group key agreement protocol makes a group of participants communicating over untrusted, open networks to arise a session key, which is a common secret value. Since there is no resources wastage while communicating nodes with another device, group key establishment is more efficient than pairwise key establishment [5].

The management of cryptographic keys in a cryptosystem is defined as key management that deals with the generation, storage, use, exchange, and replacement of keys. Key management has key servers, user procedures, cryptographic protocol design, and other relevant protocols [14]. For secure group communication systems, group key management acts as a fundamental building block. The challenges are methods for efficiently generating the secure key and re-keying, thereby maintaining the storage and communication overhead [6].

In wireless networks, group communication can be affected by illegal overhearing (e.g., packet sniffing). Secure group communication is provided by sharing a common secret key called group key for confidentiality of group messages with data encryption when a group operates with sensitive information. There is a need to decide the method for sharing a key among group members and for updating the group key for group membership change. This typical approach depends on centralized key distribution with a trusted third party and offers scalable group key management for large groups with the help of symmetric encryption, namely, hierarchical logical key tree and advanced encryption standard (AES) [7].

ISSN: 2233-7857 IJFGCN

2. Existing Survey on Key Management in MANET

Reham Abdellatif Abouhogail [1] has proposed a hybrid group key management protocol by dividing the members into clusters. It assumes a maximum allowed number of members in each cluster, thereby minimizing the required number of encryption and decryption operations for joining nodes in the cluster. This is most suitable for MANETs. This protocol is a scalable and hybrid group key management protocol in MANET to divide the multicast group dynamically into clusters. But this work concentrated mainly on wired networks.

Nagaraja *et al* [2] have surveyed the group key management by discussing about the objectives, state-of-the-art frameworks, their pros and cons and also future challenges in MANETs. But they did not provide very detailed discussion and comparative study.

M. El-Bashary *et al* [3] have surveyed several approaches in group key management schemes and compared these schemes in terms of computational complexity, reliability, communication overheads, storage cost, security levels, pre-requirements, robustness, scalability, vulnerabilities, mobility, and energy. Lastly, the pros and cons of each protocol are discussed. But only limited number of works has been discussed in this survey.

3. Survey of Key Management Techniques

3.1 Centralized Group Key Management Techniques

Luca Veltri *et al* [4] have proposed a new centralized approach for efficiently distributing and managing a group key in generic ad hoc networks and Internet of Things. Owing to group membership changes caused by users' joins and leaves, this approach minimizes the computational overhead and network traffic. Particularly, this protocol has been considered at a pre-determined time selected when the user joins the group and at an unpredictable time in case of membership revocation. A MKD protocol tailored for very dynamic ad hoc networks, which is either wired or wireless, is proposed. Time can be divided into fixed intervals in such a way that each of them is associated with a different group key. Each node shall wait until the beginning of the next slot before becoming a group member when a user can join anytime asynchronously. This introduces a delay, which is equal to half of the slot interval, but reduces the number of rekeying acts. The protocol offers proper mechanisms for managing unpredictable leave events and resisting against collusive attacks.

Xinyu Lei *et al* [5] have provided a spanning tree (ST)-based centralized group key agreement protocol for unbalanced MANETs. A local spanning tree (LST)-based distributed protocol is subsequently presented on the basis of the centralized solution. Some of the basic features of the HSK scheme followed by both protocols are discussed below. H denotes the hybrid approach is exploited; this is the combination of key agreement and key distribution via symmetric encryption; S denotes a ST or LSTs that are adopted to form a connected network topology; K denotes the extended Kruskal algorithm that is employed to handle dynamic events. For handling the initial key establishment process and all kinds of dynamic events in group key agreement protocol, HSK scheme is a uniform approach. Moreover, to reduce the overhead, the extended Kruskal algorithm realizes the reusability of the precomputed secure links. Moreover, aspects like the network topology, connectivity, and security are well analyzed. The main contributions of their proposed approach are as follow.

1) The weight function is introduced which jointly considers high communication efficiency and energy balance.

2) Hybrid encryption technique applies the symmetric encryption algorithm which is regarded to be more efficient than asymmetric encryption algorithm.

3) The extended Kruskal algorithm is very efficient to handle dynamic events. All kinds of dynamic events are well addressed by only one uniform algorithm, whereas other approaches always involve in designing several sophisticated algorithms to handle different kinds of dynamic events.

4) The extended Kruskal algorithm enables to realize the reusability of the pre computed secure links, and thus reduces the overhead.

5) There is no global broadcast in the proposed protocols. That is to say, all transmissions are based on one-hop transmission.

Yanji Piao *et al* [6] have proposed polynomial-based key management schemes. Without any encryption/decryption, group members and the group controller share the intragroup key. The group controller updates and distributes the renewed group keys when the members of the group get changed. It reduces the number of re-keying messages and lessens the storage overhead of group members and the group controller by adopting a polynomial-based key management scheme. Encryption/decryption mechanisms are not used for sharing the intragroup key between the group controller and group members. The keys are renewed immediately when membership changes happen. The adoption of the polynomial for deriving an intragroup key reduces the key storage overhead at the group members and the group controller. The members self-generate the polynomial functions needed for creating an inter-group key after the intragroup key is derived.

Sukin Kang *et al* [7] have proposed a group key sharing scheme and efficient re-keying methods for frequent membership changes from network dynamics, thereby making the group members establishing a group key and providing high flexibility for dynamic group changes such as member join or leave and group merging or partition. They investigated secure group key distribution and management for collaborative groups with high group flexibility. A DH-based group key management protocol is proposed. They showed security proof of this scheme and mathematical evaluation with other GKA protocols.

Weichao Wang *et al* [8] have proposed a mechanism that integrates polynomials with stateless secret updates for achieving personal key share distribution and efficient key refreshment during group changes. This mechanism distributes keys via true broadcast. This mechanism has the following advantages when compared to previous approaches. The limited processing capability of wireless nodes is matched by the adoption of symmetric encryption/decryption for multicast traffic matches. The properties of mobile wireless networks including frequent topology changes and temporary connection disruptions re matched by the stateless feature of key distribution. For reducing the communication overhead during key updates and providing protection against both intragroup and intergroup impersonation, special mechanisms are designed. They investigated storage, computation, and communication overhead of this mechanism.

Table 1. Centralized Group Key Management Techniques

Authors	Title	Advantages
Luca Veltri *et al*	A novel batch-based group key management protocol applied to the Internet of Things	Provides group-level confidentiality and integrity, together with per-node authentication and non-repudiation.
Xinyu Lei *et al*	Group Key Agreement Protocol for MANETs Based on HSK Scheme	Achieves high efficiency
Yanji Piao *et al*	Polynomial-based key management for secure intra-group and inter-group communication	Reduce the number of re-keying messages, lessens the storage overhead
Sukin Kang *et al*	Secure Collaborative Key Management for Dynamic Groups in Mobile Networks	Can be adapted efficiently for multicast security in mobile networks.
Weichao Wang and Tylor Stransky	Stateless key distribution for secure intra and inter-group multicast in mobile wireless network	Reduces communication overhead, provide protection against both intra and inter-group impersonation.

3.2 Distributed Group Key Management Techniques

Maria Striki *et al* [9] have adapted TGDH to be possible in the several resource-constrained MANET in which none of the nodes has special capabilities, to create significantly lower overhead for nodes involved in the network, and to manage disruptions with minimum cost. The underlying routing protocol is considered in their design. A distributed TGDH version is applied over a robust schedule by optimizing the required parameters. It is assumed that a path between group members includes nonmember relays. This protocol depends on the routing redundancy for delivering the exchanged messages in a timely manner. Dividing such group into subgroups that corresponds to a complete members' graph, reachable by the subgroup leader through a single broadcast, allows the execution of the original TGDH by the considering the aforementioned assumptions. For a large group, this approach is impractical as several subgroups will be created, subgroups are sensitive to subtle variations in mobility, and subgroups contain very few members, even a single one. Still, subgroups in close proximity cannot be merged. This results in a considerable waste in network resources, and impossible execution of Hypercube. An adaptation of TGDH has been presented to satisfy the requirements of MANET. Particularly, TGDH is modified in such a way that it is distributed, that is, there is no single point of failure leader; under a topologically aware consideration, it is executed on a schedule that optimizes their own defined routing and robustness metrics; it tolerates disruptions and failures with minimum cost; and it is more efficient in terms of computation overhead and bandwidth. This scheme is called as distributed TGDH with schedule. They evaluated both protocols under the new assumptions.

Xingwen Zhao *et al* [10] have described dynamic asymmetric group key agreement (DASGKA) without central management. This agreement combines the conventional

group key agreement, a public key encryption, and a multisignature. Their construction is same as that of the authenticated group key agreement for dynamic group. A corresponding public key is published to outsiders after a shared private key is computed. A multisignature is attached in order for outsiders to trust the public key. A detailed instance with constant rounds of interactions and constant transmission cost for each participant are discussed.

Eric Ke Wang *et al* [11] have proposed a location-based distributed group key agreement (LDGKA) scheme for VANETs that uses a hybrid approach where members in the VANET to form several logic groups in the identical region. Virtual key tree model is used within each group in order that the rekeying operation can be performed efficiently in case of joining and leaving of members. A protocol is designed for establishing the secure temporary channel dynamically for the nodes belongs to different regions. There is no need for third parties or trusted central authority. While performing any re-keying operation, a tree structure is used for decreasing the computation. Central entity that is a single point of failure or causes the performance bottleneck is not needed.

Xixiang Lv *et al* [12] have proposed a Chinese Remainder Theorem (CRT)–based secure group communication scheme for simultaneously offering confidentiality service and nonrepudiation service. All group members contribute their own public keys to negotiate a shared encryption public key corresponding to all decryption keys. In the negotiation protocol, public key is broadcasted by each group member. A common value called encryption public key is obtained by combining all the public keys on the basis of CRT. This protocol has one round with no policy administrator. The encryption public key encrypts group message. By using their own secret keys, corresponding cipher text can be decrypted by all group members.

Xiao Wang *et al*. [13] have proposed a group key management protocol with high energy efficiency for the strategic mobile scenario of MANETs. This protocol is provided with three functions to address some of the issues of improving security and energy efficiency performance. This issues are discussed as follows: (1) a self-organized group establishing algorithm is designed for strategy mobile application scenarios ensuring the stable groups regardless of users' mobility with reduced rekeying cost, (2) a lightweight contributory key agreement and authentication mechanism is proposed based on the group Diffie-Hellman protocol to improve global security, and (3) a strategic mobile management mechanism is discussed based on the Prufer codec method to manage the effect of mobility impacts for improving the multicast energy efficiency and providing secret communication among roaming users.

Table 2. Distributed Group Key Management Techniques

Authors	**Title**	**Advantages**
Maria Striki *et al*	A Robust, Distributed TGDH-based Scheme for Secure Group Communications in MANET	Produce lower overhead, handle disruptions with low cost.
Xingwen Zhao *et al*	Dynamic asymmetric group key agreement for ad hoc networks	Flexible as it can adopt other dynamic group key agreement techniques.
Eric Ke Wang *et al*	Location-Based Distributed Group Key Agreement Scheme for Vehicular Ad Hoc Network	Low computation and communication overhead.
Xixiang Lv and Hui Li	Secure group communication with both confidentiality and non-repudiation for mobile ad-hoc networks	Suitable to other network models and scenarios.

Xiao Wang *et al*	The energy-efficient group key management protocol for strategic mobile scenario of MANETs	Reduces cost of rekeying operation, enhances global security, enhance the multicast energy efficiency

3.3 Hierarchical or Tree based Group Key Management Techniques

Uday Pratap Singh *et al* [14] have proposed a distributed hierarchical group key management approach. This approach utilizes elliptic curve cryptography and hash function for securing this generation and distributing the group key. For exchange key between leaf nodes, this hierarchical key management uses elliptic curve cryptography that offers greater security with small key size. Scalar multiplication is computationally fast. Therefore, this protocol will provide more suitable and efficient technique for key management.

The basic characteristics of ECDHSA are,

1. The leaf key in the key tree is the public key of the corresponding group member, and all intermediate node keys are symmetric keys.

2. The public key of each member along with binary code the corresponding parent node is stored in a list shared by group members. This list will be updated on each membership change and from time to time.

3. All group members have the same capability and are equally trusted and equally responsible for group key generation.

Hua-Yi Lin *et al* [15] have proposed a dynamic multicast height-balanced group key agreement. In a multicast group, for efficiently and dynamically composing the group key and securely delivering multicast data from a multicast source to the other multicast group users, this agreement makes the user. The hierarchical structure of this agreement partitions the group members into location-based clusters that can reduce the communication cost and manage key when member joins or leave networks. On the basis of elliptic curve Diffie-Hellman cryptography key management, this scheme offers effective and efficient dynamic group key reconstructions, secures multicast data transmissions, fits the robustness of networks, and lowers overhead costs of security management.

Ayman EL-SAYED [16] has proposed a Hierarchical, Simple, Efficient and Scalable Group Key (HSESGK), which is a new group key management schemes, on basis of clustering management scheme for MANETs. They classified several other schemes. Group members deduce the group key in a distributed manner. This scheme contains two levels. First level is used for all coordinators of the clusters called as cluster head (CH), whereas second level for the members in a cluster with its cluster head. Two secret keys are obtained in a distributed manner: one among all the CHs and another among cluster's members and its CH. For providing robustness and avoiding fault tolerance, HSESGK uses double trees in each cluster. Group key management ensures scalable and efficient key delivery by considering the node mobility.

Jin-Hee Choa *et al* [17] have proposed adaptive intrusion detection technique on the basis of majority voting by nodes in a geographical region to solve the problem of compromised nodes' collusion. This technique considers that each node is preloaded with anomaly-based or misuse-based intrusion detection techniques for diagnosing compromised nodes in the same region. They identified the optimal intrusion detection rate and the optimal regional area size under which the mean time to security failure of the system is increased and/or the total communication cost is decreased for GCSs, given a set of parameter values characterizing operational and environmental conditions.

Jin-Hee Choa *et al* [18] have proposed a scalable and efficient region-based group key management protocol for securing group communications. They considered a region-based approach for providing scalability and dynamic re-configurability. Through this

approach, group members are broken into region-based subgroups. In order to agree on a group key in response to membership change and member mobility-induced events, leaders in subgroups communicate with each other securely. A new approach is proposed to identify the optimal setting of the region-based key management protocol, thereby improving the system's performance. They meet the secrecy requirements for secure group communication. An optimal region size is existed to minimize the network traffic by efficiently trading inter-regional versus intraregional group key management overheads.

Table 3. Hierarchical Group Key Management Techniques

Authors	Title	Advantages
Uday Pratap Singh and Rajkumar Singh Rathore	Distributed Hierarchical Group Key Management using Elliptic Curve and Hash Function	Provides much stronger security with smaller key size.
Hua-Yi Lin *et al*	Efficient Key Agreements in Dynamic Multicast Height Balanced Tree for Secure Multicast Communications in Ad Hoc Networks	Performs very well for dynamic nodes joining or leaving.
Ayman EL-SAYED	A new Hierarchical Group Key Management based on Clustering Scheme for Mobile Ad Hoc Networks	Ensure scalable and efficient key delivery.
Jin-Hee Choa *et al*	Performance analysis of hierarchical group key management integrated with adaptive intrusion detection in mobile ad hoc networks	Achieves good security level and uses less computational power.
Jin-Hee Choa *et al*	Performance optimization of region-based group key management in mobile ad hoc networks	Reduces over all network traffic.

4. Conclusion

In this survey, the detailed study about group key management techniques and its advantages and disadvantages are explained. The subsection 3.1 explains about the central group key management techniques and its advantages and disadvantages. Section 3.2 explains about the distributed group key management techniques, and Section 3.3 explains about the hierarchical group key management techniques and its advantages and drawbacks. From the survey study, we studied detail information about different group key management techniques, advantages, and disadvantages.

References

[1] Reham Abdellatif Abouhogail, "Security Assesment for Key Management in Mobile Ad Hoc Networks", *International Journal of Security and its Applications*,Vol-8,pp:169-182,2014.
[2] G Nagaraja and Pradeep Reddy CH, "A SURVEY ON GROUP KEY MANAGEMENT FRAMEWORKS FOR SECURE GROUP COMMUNICATION IN MOBILE AD HOC NETWORKS",*International Journal Of Pharmacy & Technology*,2016.
[3] M. El-Bashary, A. Abdelhafez and W. Anis, "A Comparative Study of Group Key Management in MANET",*Int. Journal of Engineering Research and Applications*, ISSN: 2248-9622, Vol. 5, Issue 8, (Part - 4), pp.85-94,2015.
[4] Luca Veltri,Simone Cirani,Stefano Busanelli and Gianluigi Ferrari, "A novel batch-based group key management protocol applied to the Internet of Things",*Elsevier,Ad Hoc Networks*,2013.

[5] Xinyu Lei, Xiaofeng Liao and Yonghong Xiong, "Group Key Agreement Protocol for MANETs Based on HSK Scheme",*IEEE*, 2013.
[6] Yanji Piao,JongUk Kima,Usman Tariq and Manpyo Honga, "Polynomial-based key management for secure intra-group and inter-group communication",*Elsevier,Computers and Mathematics with Applications*,2012.
[7] Sukin Kang, Cheongmin Ji, andManpyo Hong, "Secure Collaborative Key Management for Dynamic Groups in Mobile Networks",*Journal of Applied Mathematics*,2014.
[8] Weichao Wang and Tylor Stransky,"Stateless key distribution for secure intra and inter-group multicast in mobile wireless network",*Computer Networks*,Vol-51,pp:4303–4321,2007.
[9] Maria Striki, John S. Baras and Kyriakos Manousakis, "A Robust, Distributed TGDH-based Scheme for Secure Group Communications in MANET",*IEEE*, 2006.
[10] Xingwen Zhao, Fangguo Zhang and Haibo Tian, "Dynamic asymmetric group key agreement for ad hoc networks", *Ad Hoc Networks*,Vol-9,pp:928–939,2011.
[11] Eric Ke Wang,Yuming Ye, and Xiaofei Xu, "Location-Based Distributed Group Key Agreement Scheme for Vehicular Ad Hoc Network",*International Journal of Distributed Sensor Networks*,2014.
[12] Xixiang Lv and Hui Li,"Secure group communication with both confidentiality and non-repudiation for mobile ad-hoc networks",*IET Information Security*,2010.
[13] Xiao Wang, Jing Yang, Zetao Li and Handong Li, "The energy-efficient group key management protocol for strategic mobile scenario of MANETs",*EURASIP Journal on Wireless Communications and Networking*,2014.
[14] Uday Pratap Singh and Rajkumar Singh Rathore, "Distributed Hierarchical Group Key Management using Elliptic Curve and Hash Function",*International Journal of Computer Applications*,Volume 61–No.19, January 2013.
[15] Hua-Yi Lin and Tzu-Chiang Chiang, "Efficient Key Agreements in DynamicMulticast Height Balanced Tree for SecureMulticast Communications in Ad Hoc Networks",*EURASIP Journal onWireless Communications and Networking*,2011.
[16] Ayman EL-SAYED,"A new Hierarchical Group Key Management based on Clustering Scheme for Mobile Ad Hoc Networks",*(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 5, No. 4, 2014.
[17] Jin-Hee Cho and Ing-Ray Chen, "Performance analysis of hierarchical group key management integrated with adaptive intrusion detection in mobile ad hoc networks",*Elsevier,Performance Evaluation*,Vol-68,pp:58–75,2011.
[18] Jin-Hee Choa, Ing-Ray Chena, Ding-Chau Wang, "Performance optimization of region-based group key management in mobile ad hoc networks",*Performance Evaluation*,Vol-65,pp:319–344,2008.

