International Journal of Engineering & Technology, 7 (4.10) (2018) 344-348

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Performance Analysis of Secure Group Key Mechanism in Mobile Ad Hoc Networks

Shanmuganthan C[1]*, Raviraj P[2]

[1]*Manonmaniam Sudaranar University, Tirunelveli, Tamilnadu, India*
[2]*Professor, GSSS Institute of Engineering and Technology for Women, Mysuru, Karnataka, India*
**Corresponding author E-mail:cshanme@yahoo.co.in*

Abstract

Mobile Ad-hoc network (MANET) is an effective network administration framework that encourages trading data between remote mobile devices, without the utilization of remote access points and base stations. Security has become a major concern in mobile ad hoc networks. Providing security is the very big challenge in MANET, due to lack of infrastructure, frequent host mobility, and unreliable wireless media. We are using cryptography techniques to provide secure communication in mobile ad hoc networks. To provide security using cryptography, key management is playing a vital role. The key management includes key generation, storage, distribution, revocation, and updating. The authorized group key distributions are the difficult task in MANET. Various types of key management protocols are symmetric, asymmetric, group and hybrid. In a group key management, when a member joins or leaves the group, it needs to generate a new key immediately to maintain authentication or secrecy. The group key management is categorized into three types such as centralized, decentralized and distributed. In this paper, we analyze the performance of different group key management protocol scheme based on some important measure like reliability, limitations, services, storage cost, scalability, intermediate operation, and vulnerabilities. Finally, different categories of key management protocols compared and the results are tabulated

Keywords: *Wireless Sensor Network, Mobile Ad hoc networks, Group key, Symmetric Key.*

1. Introduction

This Mobile Ad hoc Networks (MANET) has just constrained assets that are associating with each other through remote connections and multi-hop routing with no appropriate infrastructure. Because of such qualities, framing the security mechanism is exceptionally troublesome in such situations. Cryptography could be a most generally utilized procedure for giving security that needs a key management scheme. MANET contains a collection of wireless devices which moves around uninhibitedly and works with each other packet. Multicasting could be a broadly utilized specialized technique for assembling arranged interchanges, for example, talk discussions, video conferencing, frequent stock updates, on-demand videos (VoD), pay per reading programs and promoting and etc. Ad hoc atmosphere with the mixture of multicast administrations [1] [2] [3] produces security infrastructure.

1.1. Key Management

The Key management incorporates key generation, distribution, and key exchange then it makes an essential piece for secure multicast communication applications. In an undeniably secure multicast communication, each part holds a key to scramble and decrypt the multicast data. On account of the exceptional conduct of the MANET, the secret key utilized for communication is got the chance to be effective at whatever point any node joins or leaves the network keeping in mind the end goal to deal with the forward and in reverse secrecy inside the network. Key management approach is to construct for the most part in light of identity key management. The build of identity frameworks initially was presented by Shamir in 1984 [1]. Boneh and Franklin [2] was presented with the essential of identity-based cryptography.

1.2. Group Key Management

The Group key is a unique key that is assigned to a group of nodes. In order to establish a group key, the group needs to create and distribute the key to all members of a group [15]. In a Group key management scheme, the key will be shared among all members of a group through multicasting. By using group key, we can perform encryption and decryption. If group members join or leave the group, the key will be changed immediately. If new members join, a group key must be created and distributed to the group. This process protects the new member to access previous information communicated within this group. This process is known as Forward Security. The same process is taken when a member leaves the group which is known as Backward Security.

Fig.1 shows the scheme of key management protocols. It can be classified into symmetric, asymmetric, group and hybrid. Group key protocol further divided into centralized, decentralized, and distributed group key management [15]. In a centralized group key management protocols, there is a group key server (KS) to manage the keys. In a distributed approach every member of a group is responsible for managing the keys. In a decentralized group key management protocols, the group is divided into subgroups and one of the node act as a cluster head. The group key shared to all nodes in a group and subgroups. The group key is known as Traffic Encryption Key (TEK).

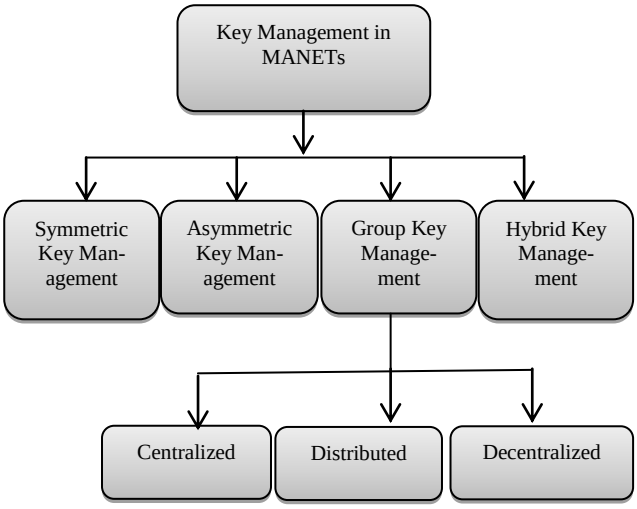

Fig. 1: Scheme of Key Management Protocol

2. Group Key Management Protocols

2.1. Simple and Efficient Group Key Management

In Simple and Efficient Group Key Management (SEGK), each group member adds to the arrangement of the common group key. This key can either be revived consistently or just when the group members change. In this method, two multicast trees work in parallel, called blue tree and red tree, which ensures adaptation to fault tolerance? On the off chance that one connection is down, it is replaced by the other tree. A group key facilitator computes and conveys the intermediate key to others nodes in the group. This node likewise keeps up the multicast group association. It is assumed that before entering the network, all the nodes have a valid certificate from an offline configuration. This implies that there is a Public Key Infrastructure (PKI) required to manage the certificates [15].

2.2. Centralized Group Key Management Protocols

The centralized group key management scheme each group consist of key server and it is responsible for key generation, distribution, and key updating. There are two variations of centralized group key management scheme called with keys pre-distribution and without keys pre-distribution.

2.2.1. With Keys Pre-Distribution

These protocols configure the hosts which will take an interest in the multicast group. This configuration is accomplished by pre-sending an arrangement of keys on every node with the goal that it will have the capacity to unscramble the multicast flow sent by the source or to get the activity encryption key. The keys pre-distribution is utilized as a part of MANETs due to the absence of networks inside mobile ad hoc networks. Two protocols have a place with this family, GKMPAN [19] and CKDS [18]. GKMPAN [26] depends on key records pre-appropriation stage to the multicast group members.

2.2.2. Without Keys Pre-Distribution

This class of protocols does not require a disconnected pre-circulation of keys. Two protocols have a place with this class, one is Kaya et al. [16] and the other one is Lazos et al. [18]. Kaya et al. propose a group key administration convention, which is effective against a few conditions forced by an ad hoc situation: portability, non-solid connections and multi-hop interchanges overhead. A certification benefit is given in this protocol, to guarantee to get to control and recognizable proof of malicious members. Just nodes with a legitimate certificate ought to have the capacity to get to the multicast flow. On the off chance that a node needs to join the multicast group it needs a security certificate got disconnected and marked by a trusted third party (TTP). Rejected nodes, with picked up certificates, ought not to have the capacity to get to the multicast information. The group members store this rundown and can validate and check the access control of each new member, needing to join the group. The key distribution process, based on the K-means algorithm shown in fig.2, is composed of the following steps:

1. Cluster Formation: All the group members assign to a cluster.
2. Subgroups: With the help of K-means algorithm divide the cluster into subgroups.
3. Refinement: Balance the group members equally into a cluster. This process is called refinement.
4. Repeat the step 2 and 3 until one or more group members created in a cluster.
5. Then Merge the cluster with one member by the pair.
6. Finally mapping the cluster hierarchy into the logical key hierarchy (LKH).

2.2.3. Leaving Probability (LP) Protocol

LP is another protocol in this centralized scheme that follows the same approach in LKH. It is used to improve the key distribution of Logical Key Hierarchy (LKH) [13] using geographical localization of the group members depends on Global Positioning System (GPS). In this scheme, members who are close to each other can receive a multicast data through the same path. The K-means clustering algorithm [14] is used to form a group with the strong correlation. It doles out the group members to a fixed number of clusters arbitrarily and afterward, changes the enrollment of the groups by expanding the connection between being the individuals from each group. The process will repeat until the assignment of the members to the clusters does not change, this means that clusters have the best geographical correlation.

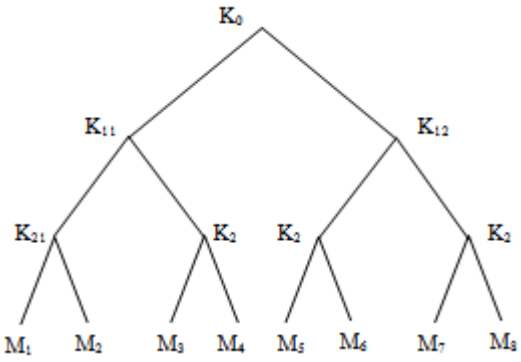

Fig. 2: Execution of K - means algorithm.

2.3. Decentralized Approach

The decentralized approach divides the multicast group into subgroups or clusters. Two sets of protocols compose this approach is called Local TEK and common TEK. In local TEK key management protocol, the multicast group is split into clusters. One of the nodes in each cluster acts as a cluster head (CH), other nodes are members of the cluster. Decentralized approach is multicast the cluster group key (CGK) between cluster head and its group members. The Key Encryption key (KEK) used to encrypt the CGK and distribute to the cluster members. In this section, we discussed two important decentralized protocols.

2.3.1. Enhanced BAAL Protocol

The Enhanced BAAL Protocol is like a BAAL protocol which provides authentication, confidentiality and access control of the nodes in the networks. There is three main component of the enhanced BAAL protocol architecture is the global controller, Local controller, and group members. The Global controller (GC) man-

ages the entire groups. The GC creates a group key and distribute to all the nodes via subgroups controllers. The role of the Local controller is distributing the group key to all the members in a group received from the group controller. The group member can join the group at any time and authentication achieved by threshold cryptography.

2.3.1. BALADE Protocol

Figure 3 shows the structure of BALADE protocol. The BALADE protocol divides the multicast node into clusters. Each cluster controlled by a local controller and all the local controllers (LC) managed by the global controller (GC). The multicast traffic is encrypted with the TEK and shared with all the group members. The group of local controller creates a multicast group called GC. Whenever a new local controller group joins, it receives the encrypted session key KEKccl from the source. The Global controller distributes TEK through multicasting to all the local controllers encrypted with KEKccl. The Local controller distributes the TEK to all the nodes encrypted with a corresponding local group key. Finally, the multicast data is decrypted only by the receiver. Only the sender can initiate the rekeying process whenever the node changes in a group.

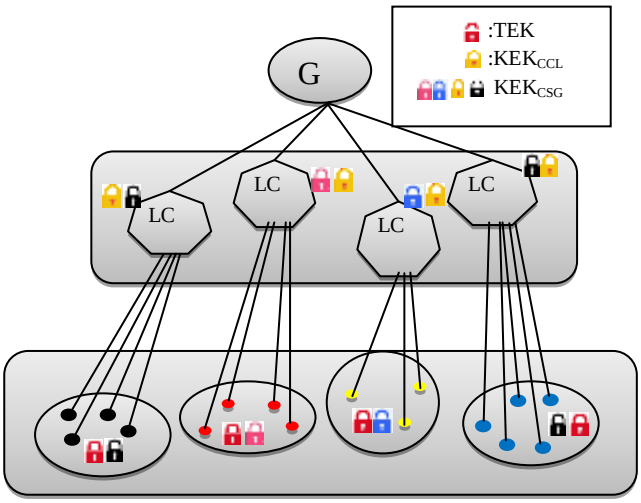

Fig. 3: Group Members Management in BLADE

2.4. Distributed Group Key Management Protocols

In this approach, all the group members responsible for generating and distributing group key for secure communications.

2.4.1. Chiang-Huang (C-H) Protocol

Chiang-Huang (C-H) proposes a group key management protocol for MANETs based on GPS data and on Group Diffie-Hellman (GDH) group key exchange protocol. During protocol initialization, each node in the mobile ad hoc network deluges its GPS information and its public key to all others nodes without the Certificate authority (CA). Based on GPS data, each node construct network topology. Prufer algorithm used to find the shortest path when a node needs to send a multicast data [19]. Prufer algorithm graph consists of K (key)-node and Leaf (U) node. K-nodes indicates key and Leaf node indicates user. The root of the key graph is called k-node. U is the set of multicast users, K is the set of keys, and P is the Prufer-key (group key).

2.4.2. ING and CLIQUES Protocol

Ingmarsson, Tang,bWang (ING) [21] and CLIQUES (CLIQ) [22], where such these two protocols are the extensions of the Diffie-Hellman (D-H) protocol [20] to n participants with a logical ordering construction. Other distributed group key protocol, which is different from the previous two protocols, is Hierarchical, Simple, Efficient, and Scalable Group Key Management (HSESGK) Protocol [23]. It provides good scalability and has efficient use under mobile conditions. This scheme, which depends on clustering algorithm and requires the certificate authority, is the adaptation of the Simple and Efficient Group Key (SEGK) scheme.

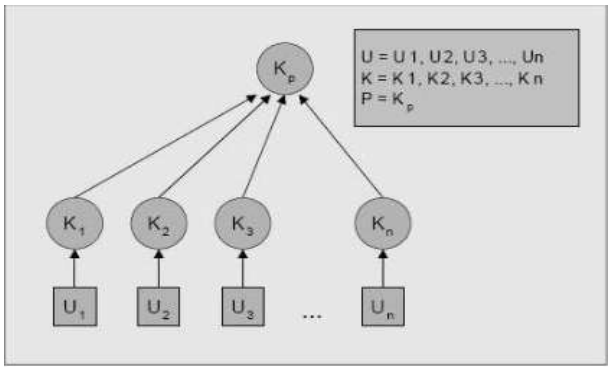

Fig. 4: A Key graphs for C-H Protocol

3. Comparison of Group Key Protocols

This section compares the differences among group key management protocols. Table 1 shows the comparison of centralized group key management protocols. The comparison is based on without pre-key distribution protocols (LKHW, Lazos and al and L-P) and with pre-key distribution protocols (GKMPAN and CKDS) scheme. Table 2 shows distributed group key protocol comparison, here we have analyzed four distributed protocols namely CH and al, ING, CLIQ, and HSESGK. Table 3 shows the decentralized group key protocols here we have compared two protocols named enhanced BAAL protocol and BALADE protocol. The comparison is based on the factors such as reliability, limitations, services, storage cost, scalability, encryption, and vulnerabilities. The reliability indicates the consistency and ability of the network topology. The limitation refers to the constraints of different group key algorithms. The services factors indicate different services like authentication, confidentiality, integrity and access control offered by the group key algorithms. The storage cost is the ability to store the energy resources. The scalability factor considers how far we can extend the key management services and vulnerability denotes the different kinds of threads and issues faced by the group key management algorithms. Finally, the intermediate operation denotes the data conversion using encryption function.

4. Performance Analysis

Here, we look at the examined protocols and break down their execution. The examined protocols are contrasted concurring with the coveted properties for multicast communications security with authentication, data confidentiality, and integrity, nodes revocation, their computational cost identified with the moderate encryption and decoding operations, their capacity cost, their effectiveness, their versatility, and vulnerabilities. GPS data is utilized as a part of Kaya et al. furthermore, Lazos et al. to productively develop ways between network nodes. The Kaya et al., Chiang et al. what's more, Lazos et al. recommendations require GPS data. Nonetheless, in Chiang et al., the GPS data is flooded inside the network enabling each group part to assemble the topology of the network. This flooding is extremely costly in impromptu networks. The Enhanced BAAL convention utilizes the edge cryptography which requires an underlying configuration in the networks. All proposed protocols which require that each group hub holds its open key. The approval of the keys records in Kaya et al. also, GKMPAN requires the TESLA confirmation. The security administrations gave the group key administration protocols incorporate information confidentiality.

Table 1: Performance Measures of Centralized Group key Protocols

	Centralized GKM					
	Without Pre-Distribution(Key)				With Pre-Distribution(Key)	
	LKHW	Lazos and al.	Kaya and al.	L-P	GKM-PAN	CKDS
Reliability	Hierarchical Tree	Hierarchical Tree	Hierarchical Tree	Hierarchical Tree	Group members share the same TEK	Group members share the same TEK
Limitations	Direct Diffusion Algorithm	K-Means Algorithm GPS	Synchronization GPS CA	Synchronization	Synchronization Predistribution	Global Controller Predistribution
Services	Authentication Confidentiality	Confidentiality	Authentication Confidentiality Access control Integrity	Authentication Confidentiality	Revocations Confidentiality	Revocations Confidentiality
Storage Cost	Keys of LKH Tree	Keys of LKH Tree	Revocation list certificates	LKH tree key distribution	Predistributed Keys	Predistributed Keys
Scalability	No	No	No	No	Yes	Yes
Intermediate Operation (Encryption)	No	No	No	No	Yes	No
Vulnerabilities	Multicast source	Multicast Source	Revocation List Updating	Multicast source	Key server	GC (Global Controller)

Table 2: Performance Measures of Distributed Group key Protocol

	Distributed GKM			
	C-H and al.	ING	CLIQ	HSESGK
Reliability	Hierarchical tree distribution based on Prufer algorithm	Ring ordering	Node ordering	Hierarchical tree distribution
Limitations	Public Key for the group nodes	Key predistribution	Key predistribution	Key predistribution
Services	Confidentiality	No	No	Data confidentiality, integrity, access control, and authentication
Storage Cost	Preferred sequence	Traffic encryption and decryption	Traffic encryption and decryption	Multicast traffic encryption and decryption
Scalability	No	No	No	Yes
Intermediate Operation (Encryption)	No	No	No	Yes
Vulnerabilities	GPS flooding and high overheads	Ring ordering and man in the middle (MIM)	Ordering, GC, and MIM	CHs

Table 3: Performance Measures of Decentralized Group key Protocol

	Decentralized GKM	
	TEKS (Local)	
	Enhanced BAAL	BALADE
Reliability	Hierarchical tree distribution and rekeying	Hierarchical tree distribution and rekeying
Limitations	Clustering Algorithm Threshold cryptography	Clustering Algorithm
Services	Authentication Confidentiality Access control	Authentication Confidentiality Access control Integrity
Storage Cost	Encryption/Decryption of multicast data by LC	KEK per cluster, Revocation The list, and ACL
Scalability	Yes	No
Intermediate Operation (Encryption)	Yes	Yes
Vulnerabilities	GC (Global Controller)	GC (Global Controller)

In any case, the confirmation and access control of the group individuals are just given by Kaya et al. what's more, Enhanced BAAL. In Kaya et al., the certification expert offers disconnected security certificates to the group individuals. The certification administration in Enhanced BAAL is accomplished through threshold cryptography, particularly to the nonattendance of any fixed framework. Nodes repudiation is guaranteed by means of the key prearrangement process in GKMPAN and CKDS. Keys of a traded off node in these two protocols will be bargained and never utilized while accomplishing the rekeying procedure. In any case, the Join technique is hard to send. Accordingly, the most reasonable arrangement in a specially appointed condition ought not to need to utilize intermediate encryption and decryption operations. The multicast information is in this manner decrypted just by the individuals, as is completed in CKDS, Kaya et al., Lazos et al., LKHW and Chiang et al. The hindrance of these conventions is that they are brought together around a substance which is in charge of the age of the movement encryption key and for the dispersion of the multicast encrypted flow. GKMPAN accomplishes encryption and decoding operations of the activity encryption key. Consequently, all the group members share a similar movement encryption key, which is circulated safely by means of the pre-conveyed keys. Notwithstanding the upsides of the dynamic grouping approach protocols are not reasonable for specially appointed systems since they utilize a nearby activity encryption key for each cluster. Therefore, these elements progress toward becoming disappointment purposes of helplessness and bottlenecks. The storage cost is additionally the primary test in specially appointed systems. Protocols having a place with the decentralized approach, Enhanced BAAL and Varadharajan et al. requires an expensive storage cost. The Prufer calculation utilized as a part of Chiang et al. likewise requires vast capacity and calculation limits, particularly for an expansive number of nodes. The capacity in Lazos et al. also, LKHW incorporate the keys of the LKH tree, though GKMPAN and CKDS store the disconnected pre-conveyed keys for every node. For GKMPAN, expanding the quantity of pre-conveyed keys m or diminishing the number of keys in the pool l will build the quantity of direct sensible ways between nodes. Be that as it may, it is alluring from the capacity perspective to diminishing m. Also, a little m and a bigger l upgrade the security level. Kaya et al. required for each group member to store its certificate and further-

more the revocation list, which ought to be refreshed by the source. A system for withdrawal of sections is utilized as a part of this rundown of revocation, however, permits denied nodes to rejoin the multicast group after a timeframe.

5. Conclusion

This paper discusses various approaches to group key management both in network independent environment and network dependent environment. The analysis shows that each protocol following various approaches like centralized, decentralized and distributed framework has its own unique features. Based on the performance measures the centralized approach is easy to implement. The de-centralized framework provides a scalable structure by dividing the participating group members into subgroups. The distributed framework allows every participating member to take part in the key management activities. The success of multicast communication relies on the security of TEK used. Thus an efficient group key management is required to generate, distribute and update the group key in a secure manner over the unsecured channel. Each category of the group key management protocol is compared based on the specific criteria and the features are tabulated. In summary, based on evaluation criteria a comparative study is conducted to show the merits and demerits of the centralized, de-centralized and distributed group key management protocols for MANETs

References

[1] HuaGuo, Yi Mu, Zhoujun Li, Xiyong Zhang," An efficient and non-interactive hierarchical key agreement protocol" Springer-Computers and Security, 2011.

[2] F. Richard Yu, Helen Tang, Peter C. Mason, and Fei Wang," A Hierarchical Identity-Based Key Management Scheme for Tactical Mobile Ad Hoc Networks", IEEE transactions on network and service management, vol. 7, no. 4, December 2010.

[3] Zainab. Zaidi, Brian L. Mark, "Mobility Tracking Based on Auto-regressive Models "IEEE transaction on mobile computing, 2009.

[4] Konstantinou.E, "Cluster-based group key agreement for wireless ad hoc networks", Third International Conference on Availability, Reliability and Security (ARES 08), March 2008, pp. 550–557.

[5] Li-Ping, Guo-Hua, Y. Zhi-Gang," An efficient group key Agreement protocol for ad hoc networks", Fourth International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '08), October 2008, pp. 1–5.

[6] Bouassida, I. Chrisment, O. Festor, "Efficient group key management protocol in MANETs using the multipoint relaying technique, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies April 2006, pp. 64–71.

[7] Li, R. Levy, M. Yu, B. Bhattacharjee," A scalable key management and clustering scheme for ad hoc networks", International Conference on Scalable Information Systems, vol.28, 2006, pp. 1–10.

[8] Rachedi A, Benslimane A, "A secure architecture for mobile ad hoc networks ", Springer's Lecture Notes in Computer Science. Hong Kong, China, December 2006. p. 424–35

[9] M. Steiner, G. Tsudik, M. Waidner," Key agreement in dynamic peer Groups", IEEE Transactions on Parallel and Distributed Systems 11 (8) (2000) pp769–780.

[10] Y. Kim, A. Perrig, G. Tsudik," Simple and fault-tolerant key agreement for dynamic collaborative groups", Proceedings of the Seventh ACM conference on Computer and Communications Security, ACM, New York, NY, USA, 2000, pp. 235–244.

[11] Zhou, Haas,"Securing ad hoc network", Technical Report, USA; 1999.

[12] M. Burmester, Y. Desmedt, "A secure and efficient conference key distribution system", Lecture Notes in Computer Science 1998, pp 275–286.

[13] M. Steiner, G. Tsudik, Waidner, "Diffie–Hellman key distribution extended to group communication", CCS '96: Proceedings of the Third ACM Conference on Computer and Communications security, 1996, pp. 31–37.

[14] Shamir A," Identity-based cryptosystems and signature schemes. Advances in Cryptology-CRYPTO'84, LNCS 196. Springer-Verlag, BerlinHeidelberg. 1984: 47−53.

[15] C.Y. Yeun, K. Han, D.L. Vo and K.J. Kim, Secure authenticated group key management protocol in the MANET environment, Information Security Technical Report, Elsevier, Vol. 13, No. 3, pp. 158-164, August 2008.

[16] T. Kaya, G. Lin, G. Noubir, and A. Yilmaz, "Secure multicast groups on Ad Hoc networks," in Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 94-102, 2003.

[17] 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.

[18] M. Moharrun, R. Mukkalamala, and M. Eltoweissy, "Ckds: An efficient combinatorial key distribution scheme for wireless Ad Hoc networks," in IEEE International Conference on Performance, Computing and Communications (IPCCC'04), pp. 631-636, Apr. 2004.

[19] S. Zhu, S. Setia, S. Xu, and S. Jajodia, GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad Hoc Networks Technical report, Feb.2004.

[20] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, pp. 644-654, Nov.1976.

[21] I. Ingemarson, D. Tang, and C. Wong, "A conference key distribution system," IEEE Transactions on Information Theory, pp.714-720, Sep. 1982.

[22] M. Steiner, G. Tsudik, and M. Waidner, "CLIQUES: A new approach to Group Key Agreement," Proceedings of ICDCS'98, 1998.

[23] A. EL-Sayed, A new hierarchical group key management based on clustering scheme for mobile ad hoc networks," International Journal of Advanced Computer Science and Applications, pp. 208-219, 2014

[24] Rafaeli, S. and Hutchison, D., A Survey of Key Management for Secure Group Communication, ACM computing Surveys, vol. 35, no. 3, pp. 309-329, 2003.