www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-1, Issue-5, Dec- 2013
Research Paper

Int. J. Sci. Res. in Network Security and Communication
ISSN: 2321-3256

Group Rekeying Management Scheme for Mobile Ad-hoc Network

Pradeep Sharma[1], Shivlal Mewada[2] and Aruna Bilavariya[*3]

[1, 2,*3]Department of Computer Science, Govt. Holkar Science College, Indore, India
aruna.bilavariya@yahoo.com

Received: 16 Nov 2013 Revised: 26 Nov 2013 Accepted: 20 Dec 2013 Published: 30 Dec 2013

Abstract- Ensuring security in Mobile Ad-hoc Network is a challenging issue Many emerging applications in mobile ad hoc networks involve group-oriented communication. In Mobile ad hoc network a mobile node operates as not only end terminal but also as an intermediate router. Therefore, a multi-hop scenario occurs for communication in network. Where there may be one or more malicious nodes in between source and destination. Establishing MANET security is entirely different from the traditional methods of providing network security. As various applications of wireless ad hoc network have been proposed, security has become one of the big research challenges and is receiving increasing attention Securing communications in resource constrained, infrastructure-less environments such as MANETs is very challenging. All cryptographic techniques will be not effective if the key management is weak. The purpose of rekeying management is to provide secure procedures for handling cryptographic keying materials. The tasks of key management include key generation, key distribution, and key maintenance. In MANETs, A number of key management schemes have been proposed for MANETs. In this paper, we proposea Centralize approach based rekeying management scheme with group management.

Keywords- MANET, Key Management, Centralized approach, Cryptography, Private Key, Rekeying System, Group Management

I. Introduction

A MANET is a special type of wireless network in which mobile hosts are connected by wireless interfaces forming a temporary network without any fixed infrastructure [1]. The combination of an ad hoc environment [2, 3] with multicast services induces new challenges towards the security infrastructure to enable acceptance and wide deployment of multicast communication. In MANET, nodes communicate each other by forming a multi-hop radio network. Mobile nodes operate as not only end terminal but also as an intermediate router. Data packets sent by a source node can reach to destination node via a number of hops. Thus multi-hop scenario occurs in communication and success of communication depends on nodes' cooperation. While mobile ad hoc networks can be quickly and inexpensively set up as needed, Security is a more critical issue compared to wire or other wireless counterparts. Many passive and active security attacks could be launched from the outside by malicious hosts or from the inside by compromised hosts [4].

A network has to achieve security requirements in terms of authentication, confidentiality, integrity, availability and non repudiation. These security requirements rely on the availability of secure key management system in network. Fundamental goal of a key management system in a network is to issue the keys to the nodes to encrypt/decrypt the messages, to manage these keys and to prevent the improper use of legally issued keys. Absence of key management system makes a network vulnerable to several attacks [5].

The principal constraints and challenges induced by the ad hoc environment are as follows.

- **Wireless Links**: The wireless links make the network easily prone to passive malicious attacks like sniffing, or active attacks like message replay or message alteration.
- **Absence of Infrastructure**: The absence of infrastructure is one of the main characteristics of ad hoc networks.
- **Autonomous**: No centralized administration entity is available to manage the operation of the different mobile nodes.
- **Dynamic topology**: Nodes are mobile and can be connected dynamically in an arbitrary manner. Links of the network vary timely and are based on the Proximity of one node to another node.
- **Device discovery** Identifying relevant newly moved in nodes and informing about their existence need

Corresponding Author: Aruna Bilavariya

dynamic update to facilitate automatic optimal route Selection.

- **Bandwidth optimization** Wireless links have significantly lower capacity than the wired links.
- **Limited Power**: Ad hoc networks are composed of low powered devices. These devices have limited energy, bandwidth and CPU, as well as low memory capacities.
- **Scalability** defined as whether the network is able to provide an acceptable level of service even in the presence of a large number of nodes.
- **Self operated** Self healing feature demands MANET should realign itself to blanket any node moving out of its range.
- **Poor Transmission Quality**: this is an inherent problem of wireless communication caused by several error sources that result in degradation of the received signal.
- **Ad hoc addressing**: Challenges in standard addressing scheme to be implemented.
- **Network configuration**: The whole MANET infrastructure is dynamic and is the reason for dynamic connection and disconnection of the variable links [6] .

The development of applications over wireless ad hoc networks is confronted by the challenge of frequent changing of environments, e.g., network topology. One approach to master this complexity lies in the grouping (clustering) of nodes over the network, i.e., applications execute on top of group services that manage the execution context dynamics, including node mobility. Another advantage of grouping in mobile ad hoc networks is to achieve system scalability, with group leaders responsible for inter-group communications. There has been extensive research on group management and related group communication services in the context of networks, with special emphasis on providing availability properties [7, 8]. However, proposed solutions cannot be applied directly to mobile wireless networks due to their highly dynamic topology [9]. This necessities the adoption of group membership to the septics of mobile networks. Group membership is primarily denned according to the functional property to be collectively achieved by the group, e.g., collaborative editing, sharing computational load, providing fault tolerance [7]. In general, a member may leave a group because it fails, explicitly requests to leave, or is expelled by other members. Similarly, a member may join a group because it explicitly les a request or recovers from failure.

II. Related Work

Recently, security has become a hot research topic in mobile ad hoc networks. Several secure routing protocols have been proposed in the literature.

In paper [2] proposed a multicast group for ad hoc network. key management scheme for MANET (Mobile Ad hoc NETworks) networks that uses asymmetric cryptography without requiring nodes to know the public keys of the other nodes and without requiring any kind of central server or certification authority.

In paper[3] proposed a hierarchical group key management scheme that is hierarchical and fully distributed with no central authority and uses a simple rekeying procedure which is suitable for large and high mobility mobile ad hoc networks. The conventional security solutions to provide key management through accessing trusted authorities or centralized servers are infeasible for this new environment since mobile ad hoc networks are characterized by the absence of any infrastructure, frequent mobility, and wireless links.

In paper [4] introduced a Secure Multicast Key Distribution for Mobile Adhoc Networks have multicast idea in mobile environment with limited bandwidth and limited power. overcome the challenging element of “1 affects n” problem which is due to high dynamicity of groups. A comparison is done against some previous technologies pertinent performance criteria.

In paper [12] propose a zone-based variant of the recently proposed cluster-based hybrid schema with an attempt to keep the advantages of the hybrid schema.

In paper [11] proposed a key management scheme and a secure routing protocol that secures on demand routing protocol such as DSR and AODV. He assumes that MANETs is divided into groups having a group leader in each group. Group leader has responsibility of key management in its group. Proposed key management scheme is a decentralized scheme that does not require any Trusted Third Party (TTP) for key management. In proposed key management system, both a new node and group leader authenticates each other mutually before joining the network.

In paper [12] proposed Group key in cryptography is a single key which is assigned only for one group of mobile nodes in MANET. For establishing a group key, group key

is creating and distributing a secret for group members. There are specifically three categories of group key protocol 1. Centralized, in which the controlling and rekeying of group is being done by one entity. 2. Distributed, group members or a mobile node which comes in group are equally responsible for making the group key, distribute the group key and also for rekeying the group. 3. Decentralized, more than one entity is responsible for making, distributing and rekeying the group key. Let us discuss about some important Group key Management schemes in MANET.

In paper [15] proposed a scheme to eliminate some reliance on TTP (Trusted Third Party), introduce distributed key pre-distribution scheme (DKPS) and construct the first DKPS prototype to realize fully distributed and self organized key pre-distribution without relying on any infrastructure support.

III. Proposed rekeying group management scheme

As we have discussed the security issues in Ad hoc networking there are many passive and active security attacks could be launched from the outside by malicious hosts or from the inside by compromised hosts.

In first type of attack or in passive attacks, an intruder captures the data without altering it. The attacker does not modify the data and does not inject additional traffic.

In second type of attack or in active attacks, an attacker actively participates in disrupting the normal operation of the network services.

1. Group rekeying management scheme:

He assumes that MANETs is divided into groups having a group leader in each group. Group leader has responsibility of key management in its group. Proposed key management scheme is a centralized scheme that does not require any Trusted Third Party (TTP) for key management. In proposed key management system, both a new node and group leader authenticates each other mutually before joining the network.

I have proposed a new method to solve some problem occur in Ad hoc networking in which we are using a concept of grouping with rekeying. The algorithm is as follow:

Step 1: Install an application at server side to encrypt incoming data every system should be connected with a centralized system called server.

Step 2: Whenever two computers want to communicate with each other they have to send data packets to centralized system (server) for making encrypted data.

Step 3: encrypted data then send to destination system.

Step 4: At the server system, proposed application install which will work grouping and rekeying.

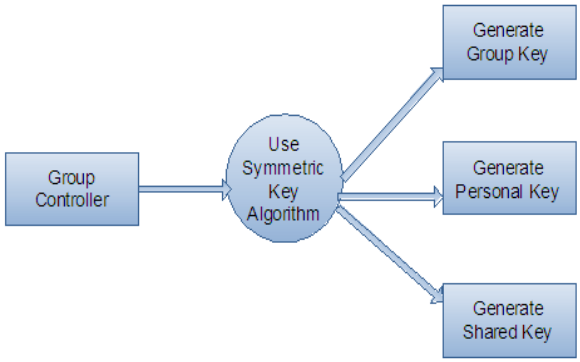

Figure 1: Working of controller (Group) on key

2. Group Management concept

Group key in cryptography technique is a single key which is assigned only for one group of mobile nodes in MANET. For establishing a group key, group key is creating and distributing a secret for group members in a particular group. There are specifically three categories of group key protocol

1. Centralized, in this type of technique the controlling and rekeying of group is being done by one entity.
2. Distributed, group members or a mobile node which comes in group are equally responsible for making the group key, then distribute the group key and also for rekeying the group.
3. Decentralized, more than one entity is responsible for making, distributing and rekeying the group key. Let us discuss about some important Group key Management schemes in MANET.

3. Rekeying concept

Rekeying normally refers to the ability to change a lock so that a different key may operate it. Rekeying is done when a lock owner may be concerned that unauthorized persons have keys to the lock, so the lock may be altered by a locksmith so that only new keys will work. Rekeying is a relatively simple a process of changing the tumbler or wafer configuration of the lock so a new key will function whiles the old one will not. Rekeying may be done without replacement of the entire lock. Rekeying was first invented in 1836 by Solomon Andrews, a New Jersey locksmith. His

lock had adjustable tumblers and keys, allowing the owner to rekey it at any time. Later in the 1850s, inventors Andrews and Newell patented removable tumblers which could be taken apart and scrambled. The keys had bits that were interchangeable, matching varying tumbler configurations. This arrangement later became the basis for combination locks.

Each member holds a key to encrypt and decrypt the multicast data. When a member joins and leaves a group, the key has to be updated and distributed to all group members in order to meet the above requirements. The process of updating the keys and distributing them to the group members is called rekeying operation. Rekeying is required in secure multicast to ensure that a new member cannot decrypt the stored multicast data (before its joining) and prevents a leaving member from eavesdropping future multicast data.

4. In Cryptography

In cryptography, **rekeying** refers to the process of changing the session key-- the encryption key of an ongoing communication -- in order to limit the amount of data encrypted with the same key. Roughly equivalent to the classical procedure of changing codes on a daily basis, the key is changed after a pre-set volume of data has been transmitted or a given period of time has passed. In contemporary systems, rekeying is implemented by forcing a new key exchange, typically through a separate protocol like internal key exchange (IKE). The procedure is handled transparently to the user. A prominent application is Wi-Fi Protected Access (WPA), the extended security protocol for wireless networks that addresses the shortcomings of its predecessor, WEP, by frequently replacing session keys through the Temporal Key Integrity Protocol (TKIP), thus defeating some well-known key recovery attacks.

Step 5: Using concept of Grouping and rekeying we can develop a system more secure than other system because we are using a concept of rekeying through which we am providing double security to encrypt key generated by encrypted data.

5. Layout of Network

Here the entire set of nodes is divided into a number of groups and the number of nodes within a group is further subdivided into subsets firstly is called clusters. Each group is managed by a group leader (g) and a cluster by the cluster's head is called cluster head. The layout of the network is as shown in Fig.1. One of the nodes in the cluster is head (h). A set of eight such clusters form a group and each group is managed by a group leader. The cluster head is similar to the nodes in the network. The nodes within a cluster are also the physical neighbors. The nodes within a cluster will handled key management. Each node within a cluster contributes his share in arriving at the group key. There will be some nodes will join the group and some will leave the group whenever membership changes occur, the adjacent node have to initiate the rekeying operation thereby reducing the overhead on the head of cluster. In the first group leader chooses a random key to be used for encrypting messages exchanged between the cluster heads and the network head sends the key to the group leaders that is used for communication among the group leaders. The hierarchical arrangement of the network is shown in figure.

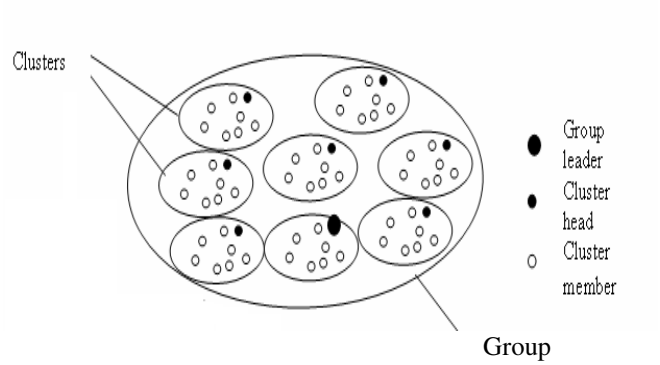

Figure 2: Network Layout

The key management system consists of two phases

(i) Initialization

(ii) Group Key Agreement

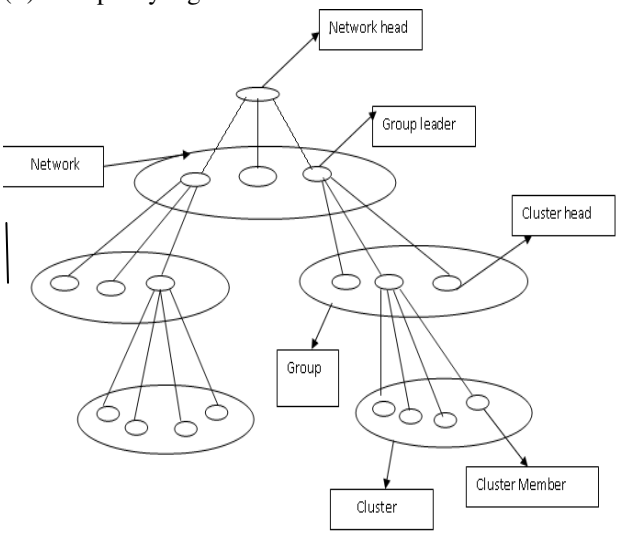

Figure 3 : Hierarchical layout

A. Initialization

Step 1: in the start nodes have to broadcast their id value to their neighbors along with the HELLO message.

Step 2: When all the nodes have found their neighbors, they exchange information about the number of one hop neighbors. The node which has maximum one hop neighbors is selected as the cluster head. And it will be cluster head. Other nodes become members of the cluster or local nodes. The nodes update the status values accordingly.

Step 3: The cluster head broadcasts the message "I am cluster head" so as to know its members.

Step 4: The members reply with the message "I am member" and in this way clusters are formed in the network.

Step 5: If a node receives more than one "I am cluster head" messages, it becomes Gateway which acts as a mediator between two clusters.

After following this manner clusters are formed in the network. The cluster heads broadcast the message, "Are there any cluster heads" so as to know each other. The cluster head with the smallest id is selected as the leader of the cluster heads which is representative of the group called the group leader. The group leaders establish communication with other group leaders in a similar manner and one among the group leaders is selected as the leader for the entire network. The entire network is hierarchical in nature and the following hierarchy is observed:

Network-> group->cluster->cluster members

B. Group Key within a cluster

Step 1: Each member broadcasts the public key along with its id to all other members of the cluster along with the identity.

Step 2: The members of the cluster generate the group key in a distributive manner but it will be just a private key. Each member operates in a random manner and THEY WILL GENERATE A HASH and will send the hash of this number these number will go to another member these members encrypted with the asymmetric key of the individual members, than using of private key anther members they don't have public key they use private key for decryption.

Step 3: which value will received by members it will be concatenates hash value in a order. it will be the generation of group key and it will be used for clusters of this group.

I am creating two or more groups and each group can communicate with each other. Member of single group also can communicate with each other. Every group has a head which is called server when a system send message to centralize system with destination address then two cases can occur.

Case 1: Communication in a Group If two system of a single group want to communicate with each other then they have to send data packet to centralize device at that server encrypted data generated with key and this key again encrypted at server. So that our data will get double security. Let us see that is a group and A an B is two nodes in figure 8 they want to communicate for communication of they have to interact to H which is a head or leader of Group G. Then node A sends data it have to send packet to H then these data will be encrypted by private key than it encrypted data will be send to node B. it will be work as single encryption . Destination node B will have cipher text than it will be decrypted by key of destination node. We can understand this case by this figure.

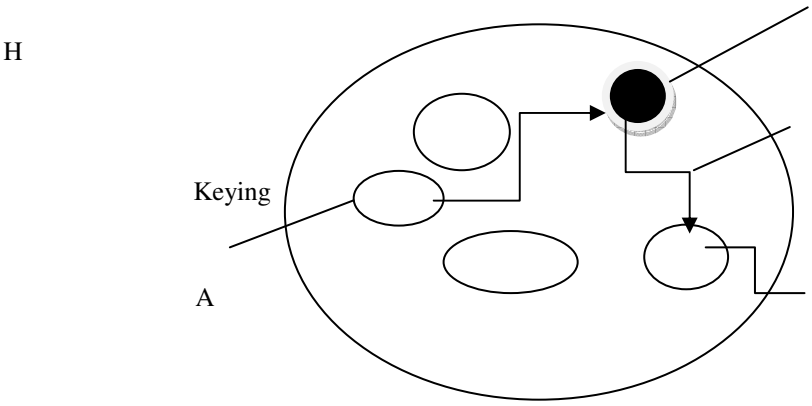

Figure 4: Communication in a Group

Case 2: Communication Between two Groups
If two system of different group want to communicate with each other then head of both groups will perform their job and generate key with rekeying. We can understand this case by the figure 9 which we have shown below There are two groups G1 and G2. They have number of nodes which can communicate with each other. For communication there are two nodes. Node A and Node B.

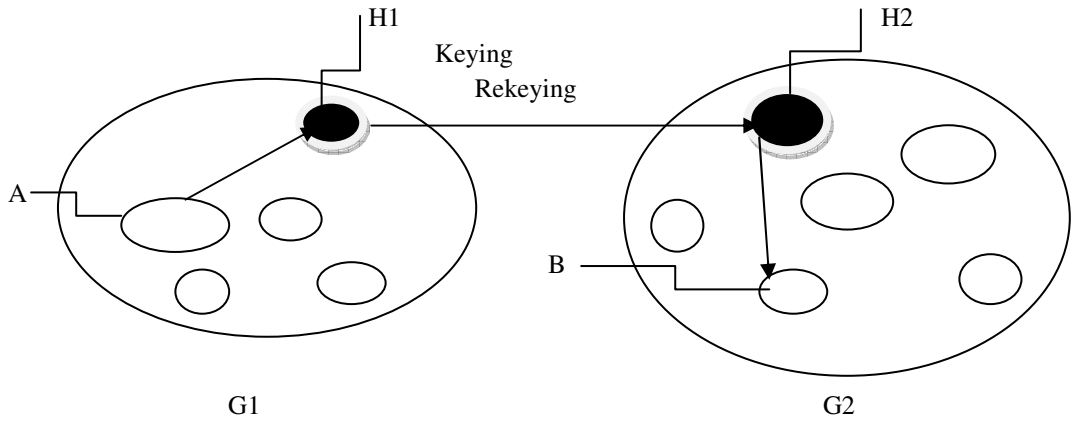

Figure 5: Communication Between two Groups

There are so many applications of MANET they require secure group communications. The MANETs are normally operated in autonomous environment. The hackers can also be compromised with some different nodes or terminals and they can misuse of shared key and they can affect the network and can break the security of network. When there is any malicious node is detected definitely group key have to renewed immediately because of maintaining security of network system .Some strategies have been proposed to develop the group rekeying schemes, but most of existing schemes are not suitable for wireless networks due to their high overhead and poor scalability. In this research, we proposed a new group rekeying scheme with group management for centralized MANETs with renewable network devices. Compared with existing schemes, our rekeying method possesses the following features that are particularly beneficial to the resource-constrained large-scale MANETs:

(1) It will be Robustness to the node capture attack,
(2) It will be Reactive rekeying capability to malicious nodes, and
(3) There will be Low communication and storage overhead.

IV. Recommendation

We have discuses principle issues of mobile ad hoc network. We have proposed a secure scheme "Group Rekeying Management Scheme for Mobile Ad hoc Network". When we use this scheme for transmission it will give write results and solve issues of security in Mobile Ad hoc Network. In this research we have surveyed the key management schemes for Mobile ad hoc networks. we gave a brief description about all the key management schemes discussed above and then a comparative survey has been made depending upon the characteristics and the features of the key management schemes. The comparative survey is carried out for the key management schemes based upon the features like Reliability, Scalability, Robustness and Security. The Analysis gave an interesting result where the Private ID based Key and Private Group Signature key Schemes performs well for Mobile ad hoc networks. Security and an effective data communication considered together due to overheads initiated by an attacker by attacking or accessing the unauthorized data in ad hoc networks.

V. Conclusion

In this research, we propose a "Group Rekeying Management Scheme in MANETs " Using symmetric key concept with centralized Approach of MANETs . Compared with existing schemes, this rekeying method possesses the following features that are particularly beneficial to the resource-constrained large-scale MANETs:

(1) Robustness to the node capture attack,
(2) Reactive rekeying capability to malicious nodes, and

(3) Low communication and storage overhead.
(4) More secure
Group management- Group leader has responsibility of key management in its group. Proposed key management scheme is a centralized scheme that does not require any Trusted Third Party (TTP) for key management.
Concepts used:

1. Group management- For security in large group
2. Rekeying- specially for inter group or 2 or more than 2 group
3. Symmetric key- using private key rekeying management in another group for different key as rekeying
4. Centralized Approach –because one entity can control rekeying in group

VI. Future work

The proposed scheme developed based on Group Key Management security groups has been formed and the communication is done based on rekeying mechanism. Group Key management is introduced for improved secure communication guided routing to nodes in MANET and for data communication security on receiving the data or sending the data to and from other mobile nodes. As the applications of mobile ad-hoc networks gain more ground, security issues becomes a good research topic. This discussed the new Group Rekeying management (GRKM) scheme which is suitable for the key management. Proposed technique addresses the network security Issues. Besides, the technique uses a key system, and consists that define how keys are centralized added, and updated during the life time of the network. In real time application that relies on wireless communication has a big issue that is network security and authentication. Therefore, providing security and authentication is important as much as providing network connection to the user. This is the major concern for most of the network service providers today and hence data encryption and proper key management techniques are very critical in enhancing the security .Future work may concentrate on cluster head that takes more some of responsibility to send secure message at the destination. This research generally discusses on various key management schemes proposed in literature. These centralized key generation techniques are based on cryptographic techniques. MANET‘s security is the challenging issue in providing authentication. Single shared key for many applications may raise problems in ensuring authentication. The approach of employing centralized key scheme for MANET ensures the network security. This research discusses on different cryptographic key generation techniques that are proposed in literature. Some of the techniques described are Symmetric Key Cryptography, Digital Certificates, and Threshold Cryptography. The future work utilizes one of the best cryptographic techniques for generation of distribution key that improves the network security in MANETs and in other wireless networks.

References

[1]. T. Chiang and Y. Huang. “Group keys and the multicast security in ad hoc networks”. In Proceedings of the 2003 International Conference on Parallel Processing Workshops, 2003.
[2]. 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, pages 94–102. ACM Press, 2003.
[3]. D.Huang, D.Medhi, “A Secure Group Key Management scheme for Hierarchical Mobile Adhoc Networks”, Adhoc Networks, June 2008.
[4]. Umesh Kumar Singh, ShivlalMewada, Lokesh Laddhani & Kamal Bunkar, “An Overview & Study of Security Issues in Mobile Ado Networks”, International Journal of Computer Science and Information Security (IJCSIS) USA, Volume-9, No.4, pp (106-111), April 2011.ISSN: 1947-5500
[5]. N. Kettaf, H. Abouaissa, P. Lorenz, “An Efficient Heterogeneous Key Management approach For Secure Multicast Communication in Ad hoc networks”, Springer, Telecommunication System, vol-37, pp: 29-36 , February 2008
[6]. Thair Khdour and Abdullah Aref, “A HYBRID SCHEMA ZONE-BASED KEY MANAGEMENTFOR MANETS”, Journal of Theoretical and Applied Information Technology, Vol. 35 No.2, 31 January 2012.
[7]. G. Chockler, I. Keidar, and R. Vitenberg. “Group communication speci_cations: A comprehensive study”. ACM Computing Surveys, 33(4), December 2001.
[8]. D. Powell. Group communication. CACM, 39(4), 1996.
[9]. C. Basile, M.-O. Killijian, and D. Powell. “A survey of dependability issues in mobile wireless networks”. Technical report, LAAS CNRS, France, February 2003.
[10]. http://citeseer.nj.nec.com/400961.html.2000.H. Dang, W. Li, and D. P. Agrawal, “Routing security in wireless ad hoc networks”, IEEE Communications Magazine, 0163-6804, pp. 70-75, October 2009.
[11]. Kamal Kumar Chauhan and Amit Kumar Singh Sanger, “Securing Mobile Ad hoc Networks: Key Management

and Routing", International Journal on Ad Hoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012.

[12]. Merin Francis, M. Sangeetha and Dr. A. Sabari, "A Survey of Key Management Technique for Secure and Reliable Data Transmission in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Issue 1, January 2013.

[13]. 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, Jan. 2008.

[14]. S.Rajarajeswari and S.BaghavathiPriya, "An Optimal key Management for MANET", International Journal of Innovations in Engineering and Technology (IJIET), Vol. 2 Issue 1 February 2013.

[15]. Aldar C-F. Chan, Edward S. Rogers, "Distributed Symmetric Key Management for Mobile Ad hoc Networks", IEEE INFOCOM ,vol.6,issue 1, feruary 2004.

[16]. Manel Guerrero Zapata, "Key management and delayed verification for Ad hoc networks", Journal of High Speed Networks 15 (2006) 93–109

