Journal of Theoretical and Applied Information Technology
20th March 2013. Vol. 49 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MULTI-LEVEL GROUP KEY MANAGEMENT TECHNIQUE FOR MULTICAST SECURITY IN MANET

[1]R.VENNILA, [2]V.DURAISAMY

[1]HOD, Department of Electrical &Electronics Engg,

Nachimuthu Polytechnic college,Pollachi

[2]Principal, Hindustan College of Engineering & Technology, Coimbatore

E-mail:[1] rvennilaphd@gmail.com

ABSTRACT

In Mobile AdHoc Networks (MANETs), data transmission is speeded up by means of multicasting. Though multicast transmission lessens overhead, collision and congestion, it persuades new challenges towards security management. This challenge must be conquered to bring better throughput of the network. In this paper, we introduce a multi level group key management technique for multicast security in MANET. Our technique works in a hierarchical model such that cluster heads are prioritized over cluster members. The secure keys are generated using one-way function chain. In addition to secure key management, the issue of mobility is also handled. By simulation results, we prove the proficiency of our proposed technique. Our secure key management technique incurs low overhead and delay and significantly increases the throughput.

Keywords: *Mobile AdHoc Networks (MANETs), Key Management, Data Transmission*

1. INTRODUCTION

1.1 Mobile Ad hoc Network (MANET)

A set of wireless communication nodes performing self-configuration in a dynamic mode for formation of network excluding fixed infrastructure or centralized supervision is termed as mobile ad hoc network (MANET). The nodes in MANET perform both as hosts as well as as routers for sending the packet to each other [1]. The network topology keeps changing quickly and randomly while the terminal connectivity changes according to time. The application of the MANET includes military battlefields, emergency search, and rescue locations etc that requires quick deployment and active re-configuration. It can also be utilized in local scenario that includes taxicab, sports, stadium, boat, small aircraft and conference hall [2].

1.2 Multicast Routing in MANET

The process of broadcasting the packets to a group of zero or more hosts recognized by a single destination address is termed as multicasting. This technique is aimed for group-oriented computing in which the host may join or leave the group irrespective of the time. A host can be member of more than one group at a time. In addition, there is no limitation for host that it should a member of a group for forwarding the data packets to the members of the respective group. While transmitting the multiple replicas of messages to utilize the broadcast nature of wireless transmission, multicasting technique is used [3].

The multicast routing protocol is involved in distributing the data from source to multiple destinations systematized in multicast group [4]. The various techniques by which the routes are generated for members of the multicast group are classified into four types namely, tree based, mesh based, stateless multicast and hybrid approaches [5, 6].

MANET is more susceptible to security threats due to their most complicated and distinctive nature [7]. The indication of the link failure or wrong message creation by the malicious node causes disconnection of the genuine node from the network or tree. The droppings of leaf nodes, alterations, repetitions, data injection or selective forwarding data after route selection are some of the attacks against data messages. In general, the categories of attacks in multicast routing are as follows [4]:

- **Denial-of-Service Attack:** The interruption caused during the delivery of packets results in denial of service attack.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The computational, sending or receiving capacities of a node are annihilated by the attacker.

- **Black Hole Attack:** During this attack, one or more attacker nodes forward only routing control packets but drops all the data packets.
- **Wormhole Attack:** The packets that are received at one point by the attacker are tunneled to another point in the network. Then the attacker repeats the process of tunneling the packet from that point into the network.
- **Flood Rushing Attack:** The attackers flood the authenticated messages through the network in prior to flooding it through a legitimate route. This action causes the adversaries to control several paths. The process of flood rushing enhances the efficiency of a black hole or wormhole attack
- **Selfish Nodes:** Certain attackers may save its own resources and start using the services of others and consumes their resources, which are described as selfish activity. These selfish nodes take part in the route discovery and maintenance phase while repudiating the data packet forwarding. This action degrades the routing performance.
- **Jellyfish Attack:** Initially jellyfish attacker interrupts the multicast-forwarding group. Further, unreasonably it delays the data packets time prior to data forwarding. Consequently, it results in high end-to-end delay [8].
- **Neighbor attack:** The intermediate node upon receiving a data packet appends its ID before forwarding it to the next node. However, if it is attacker, then it just forwards the packet without its ID. This causes two nodes apart from each other to believe that they are neighbors resulting in a disrupted route [8].

1.3 Key Management

For group communication applications, the process of generating, allocating and updating keys plays an important role and the entire process is termed as key management. The key management process strives for point towards secure distribution of keying materials [9]. For the most part, the security services use Traffic Encryption Keys (TEKs) for encryption and Key Encryption Keys (KEKs) for decryption. This key is maintained by the mobile node for encrypting and decrypting the multicast data. Whenever a node joins and leaves a group, this key has to be updated and distributed to all nodes regularly [10].

During data transmission, the energy consumed by each node is an important, since the nodes in MANET contain limited battery power. This issue has to be considered mainly in the process of key management. However, generating, distributing and updating keys require more energy and needs energy efficient approaches [10].

In MANET, message delivery can be speeded up by means of group communication and it alleviates the consumption of more bandwidth during transmission. On the contrary, the group communication brings in many challenges as the data is transmitted over a general tunnel without any security mechanisms such as encryption. Further, this paves way for more malicious attacks. Consequently, these attacks affect the internet significantly [9].

The mobility of nodes extremely affects the process of key management. In addition, when nodes move from one group to another, it incurs more overhead and consumption cost [11].

1.4 Problem Identification

In our previous work [12], we have proposed a QoS based clustering technique for multicast security in MANET. In this technique, the nodes with maximum available bandwidth and residual energy are elected as cluster heads, which act as multicast group leaders. Each cluster head computes the trust value of its members using success or failure ratio of data and control packets. Based on the trust value, the cluster head decides whether a node is authorized to join the multicast group or not. When the multicast source wants to transmit the data packet, it utilizes the secret key-based packet forwarding technique.

The proposed secure transmission mechanism technique cannot be applied to multi-level and multi key structure. In order to provide an efficient secure mechanism for multi level and multi key structure, in this paper we propose to design a multi-level group key management technique for multicast security in MANET

2. RELATED WORKS

Nen-Chung Wang et al. [9] have proposed a hierarchical key management scheme called HKMS for secure group communications in MANETs. For

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the sake of security, their approach encrypts the packet twice. They generate an L1-subgroup key for each L1-subgroup and an L2-subgroup key for each L2-subgroup. The procedure of delivery is to encrypt the packet firstly by private key, and then encrypt and decrypt it again by L1-subgroup key and L2-subgroup key. The disadvantage of the proposed scheme is that, the maintenance cost increases when group membership increases.

Pavithira Loganathan et al. [10] have proposed an energy efficient topology aware key management scheme. Their proposed scheme includes a temporary key tree construction algorithm. It has reduced the re-keying load by pre-processing the joining members during the idle re-keying interval. Re-keying is required in secure multicast communication to ensure that a new member cannot decrypt the stored multicast data (before it joining) and prevents a leaving member from leaves dropping future multicast data. The energy expenditure for key distribution is reduced by assigning common keys to members, which are physically close. The temporary key tree algorithm significantly reduces both computation and communication costs.

Dijiang Huang et al. [11] have proposed a secure group key management scheme for hierarchical mobile ad-hoc networks. Their approach has considered Bell-La Padula, a multi-level security model and a hierarchical group-keying scheme using a key-chain approach. Their approach has reduced the key management overhead and improved resilience to any single point failure problem. In addition, they have developed a roaming protocol that is able to provide secure group communication involving group members from different groups without requiring new keys. However, with the increases in the number of groups and the height of the hierarchical structure, the communication overhead and the key derivative complexity do increase.

Mohamed-Salah Bouassida et al. [13] have proposed BALADE, which is a group key management protocol for ad hoc environments. Their BALADE is to secure multicast communications, according to the sequential multi-sources model. Their proposed approach is based on the dynamic clustering approach, using one traffic encryption key, and several key encryption keys, thus eliminating the overhead induced by the intermediate encryption and decryption operations on the multicast flow. It uses the OMCT (Optimized Multicast Cluster Tree) algorithm to ensure an efficient and fast group key delivery.

Hua-Yi Lin et al. [14] have proposed a dynamic multicast height balanced group key agreement termed as DMHBGKA. Their proposed approach allows a user in a multicast group to efficiently and dynamically compose the group key and securely deliver multicast data from a multicast source to the other multicast group users in wireless ad hoc networks. The hierarchical structure of key agreement partitions the group members into location-based clusters capable of reducing the cost of communication and key management when member joins or leave networks. Furthermore, their approach has utilized Elliptic curve Diffie–Hellman (ECDH) key operations and a rapid hash function for secure multicast data transmission and data integrity verifications.

Attila A.Yavuz et al. [15] have proposed a new multi-tier adaptive military MANET security protocol. Their security protocol has used hybrid cryptography and signcryption. For securing data transmission, they have used hybrid cryptography mechanisms and Elliptic Curve Pintsov-Vanstone Signature Scheme (ECPVSS). Their security approach has provided adaptive solutions according to the requirements of different military units in the MANET. They have also used a hybrid key management technique that combines the benefits of both decentralized protocols with single point of failure resistivity and centralized protocols with low rekeying cost.

N. Vimala et al. [16] have proposed a region-based group key management protocol. Their region-based group key management protocol divides a group into region-based subgroups based on decentralized key management principles by using the Novel Re-Keying Function Protocol (NRFP). This partitioning of region into subgroups improves scalability and efficiency of the key management scheme in providing a secure group communication. Their scheme has employed an MDS code, which is a class of error control codes, to distribute multicast key dynamically.

3. MULTI LEVEL GROUP KEY MANAGEMENT TECHNIQUE

3.1 Overview

In this paper, we propose to deploy a multi level group key management technique for multicast security in MANET. Our technique works in a hierarchical model such that cluster heads are prioritized over cluster members. Initially, after the nodes are deployed in the network, node with high bandwidth and residual energy is elected as cluster

Journal of Theoretical and Applied Information Technology
20th March 2013. Vol. 49 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

head. Once the cluster is formed, each cluster head (CH_i) generates a set of keys for its cluster members. Keys are generated using one-way function chain. The generated keys are distributed to the cluster members using shuffle algorithm. Similarly, the source generates and distributes secret keys to the CH_i. While data is transmitted from the multicast source to the destination; the source encrypts the message using its shared key with CH_i and forwards to the cluster head. The CH_i decrypts the message using its shared key with source and encrypts again with shared secret key of cluster member. Apart from this secure transmission, our technique has considered the issue of mobility of nodes. The mobility management is achieved by means of Prufer algorithm.

3.2 Network Architecture

After the distribution of nodes in the network, each node measures its available bandwidth and residual energy. These values are broadcasted in the network through cluster request (CREQ) message. The node with high bandwidth and residual energy is elected as cluster head. The network architecture of our proposed technique is shown below in figure-1.

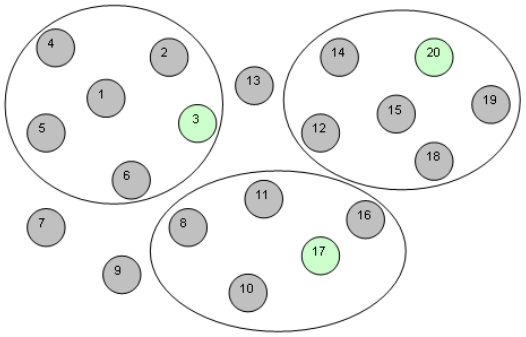

Figure-1 Network Architecture

The steps involved in clustering are as follows

1) Initially after the deployment, each node (N_i) in the network broadcasts cluster request (CREQ) message to its neighboring nodes (N_{neighi}).

$$\text{Node } N_i \xrightarrow{CREQ} N_{neighi}$$

2) Upon receiving CREQ, N_{neighi} constructs the cluster reply (CREP) message that includes the information about the available bandwidth and residual energy of the node. Then it sends the reply message to the requested node N_i.

$$\text{CREP: } (AB_i + RE_i)$$

$$\text{Node } N_i \xleftarrow{CREP} N_{neighi}$$

3) Among the nodes that send the CREP message, the nodes with the higher value of available bandwidth and residual energy is chosen as cluster head (CH) by other nodes and remaining nodes becomes the cluster members (CM).

4) The CH then sends a declaration message to all its members that it has been selected as cluster head through a hello message.

$$CH_i \xrightarrow{HELLO} CM_i$$

5) CH acts as the multicast group leaders (GL) and multicast data (MD) is transmitted from the source (S) to the group members (GM) through the corresponding GL.

3.3 Multilevel Secure Key Management Technique

Our multilevel secure key management technique works in a hierarchical way such that cluster heads (CH) are prioritized over cluster members. We assume that each mobile node in the network is preinstalled with same set of secret keys.

3.3.1 Generating keys using one way function chain

Once the cluster is formed in the network, the CH generates secure keys for their group members using one-way function (OFC) chain [17].

This initial key generation is done with one- way function (OFC). The OFC is a function, which is easy to encode and difficult to invert. By means of one- way function, each node forms a key chain. This function is used to fabricate the keys and consequently develops a key chain. The OFC produces a set of keys using a sequence of values along with their linear derivation relations.

Consider a function OF is recursively applied j times to an argument n, that is $OF^j(n)$, then it can derive $OF^i(n)$ provided $j < i$. Let $K_{x0} = I_x$ be the x-th initial key element to originate a set of secret keys. A secret key K_{xy} is denoted by,

$$K_{xy} = f\ (OF^j(I_x)) \quad (1)$$

Where, f is the universal key generating function. Using above described considerations, the OFC generates the following derivative relations that is key chain as,

$$K_{x0} \rightarrow K_{x1} \ldots \rightarrow K_{xy} \rightarrow \ldots \rightarrow K_{xi} \text{ where } 1 < j < i \quad (2)$$

Journal of Theoretical and Applied Information Technology
20th March 2013. Vol. 49 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The following figure-2 shows the one-way function chain of derivative described in equation (2)

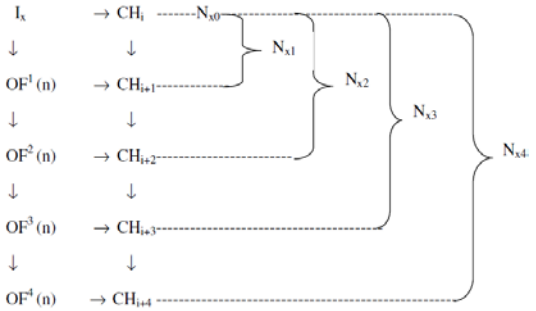

Figure 2 : One Way Function Chain

Where CH_i, CH_{i+1}, CH_{i+2}, CH_{i+3} and CH_{i+4} are symbolized the cluster heads and N_{x0} ...N_{x4} are the lower level nodes that is cluster members. Each CH derives its key and keys for their group members. For n nodes in the network, keys are distributed to them from $\frac{n(n+1)}{2}$ key chains. OFC enables our technique to manipulate hierarchical key structure. Thus, using predistributed keys, each CH obtains the keys for its cluster members.

3.3.2 Key distribution using shuffle algorithm

Each cluster head (CH_i) in the network produces the secret keys for its cluster members using predistributed keys as we discuss in section (3.4). After the generation of keys, they are distributed to each member of the cluster using shuffle algorithm. The shuffle algorithm is as follows,

Algorithm-1

Let CH_i be the cluster heads, i = 1,2,…n and K_{CHi} be the predistributed keys of cluster head CH_i

Input: $\{K\}_{CHi} = \{K_1 \ldots K_{x0}, \ldots, K_n\}$, where $1 \le x \le n$

1. Start
2. y = 1
3. For ($k'_{y0} = OF(k_{x0}, k_y)$)
4. If (y == n) Goto step-7 End if
5. y = y +1
6. Goto step-3
7. Stop

Output: $\{k'\}_{CHi} = \{k'_{10}, \ldots, k'_{x0}, \ldots, k'_{n0}\}$

The shuffle algorithm takes $\{k\}_{CHi}$ as an input, which is the existing key set and produces $\{k'\}_{CHi}$ as the output, new key set.

Consider the network architecture given in figure-1, in that node 3, 20 and 17 are the cluster heads. The cluster head 3 has 1, 2, 4, 5 and 6 as its cluster members. Consider that CH3 generates and distributes the key to their cluster members using one way key function and shuffle algorithm respectively. The schematic diagram of key generation and distribution is shown below in figure-3. In that representation, the input is denoted as {K} and the output as {K'}. The predistributed keys of CH3 are taken as inputs to the one-way function chain and the generated keys are distributed to its cluster members CM1, CM2, CM4, CM5 and CM6 using shuffle algorithm. OF symbolizes the global one-way function.

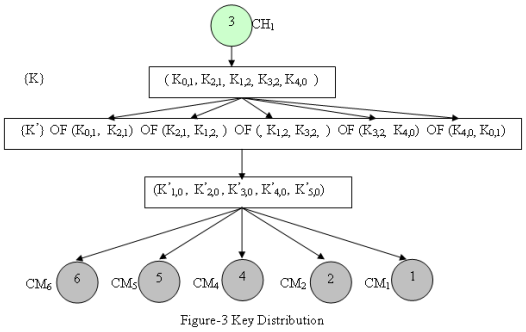

Figure-3 Key Distribution

In similar to key generation of CH_i, the multicast source (S) derives unique key set as follows,

1) The multicast source forwards its predistributed keys as input to the OFC
2) As an outcome of OFC, the multicast source retrieves a set of key for all cluster heads. Here, the multicast source is prioritized over cluster heads CH_i.
3) It then distributes the generated keys to CH_i using shuffle algorithm

Now, each CH_i shares a unique symmetric key with its members and the multicast source shares unique key with all CH_i.

3.3.3 Secure data transmission

Let $K_{SCH(i)}$ be the secret key distributed by multicast source S to CH_i and let ($K_{MCH(i)}$) be the secret key generated by CH_i and distributed with its cluster members (CM_i). The multicast source S and the CH_i generates and distributes key using OFC and shuffle algorithm respectively.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

When the multicast source (S) wants to transmit multicast data, it first encrypts the data with $K_{SCH(i)}$, appends its ID_S and message authentication code (MAC ($K_{SCH(i)}$, d_S)) to the encrypted data and sends it to the respective CH_i. The format of the data forwarded is as follows

$S \rightarrow CH_i$: ID_S | Encr ($K_{SCH(i)}$, d_S) | MAC ($K_{SCH(i)}$, ID_S |Encr ($K_{SCH(i)}$, d_S))
Where ID_S = source ID.
d_S = data arriving from the multicast source.

The data is encrypted in order to maintain the data confidentiality. The encrypted data is appended with message authentication code (MAC) to assure the message authenticity.

The CH_i upon receiving the data decrypts it using $K_{SCH(i)}$ and extracts the data. CH verifies whether the MAC is valid. If it is valid, then CH_i re-encrypts the data with $K_{MCH(i)}$ and delivers it to the respective cluster member (CM_i).

CH_i: ID_S| Decr ($K_{SCH(i)}$, d_S) | MAC ($K_{SCH(i)}$, DATA |ID_S | Decr ($K_{SCH(i)}$, d_S))
$CH_i \rightarrow CM_i$: ID_{CHi}| E ($K_{MCH(i)}$, d_{CHi}) | MAC ($K_{MCH(i)}$, DATA |ID_S |E ($K_{MCH(i)}$, d_{CHi}))
Where ID_{Chi} = cluster heads ID
d_{Chi} = data arriving from the cluster head.
CM_i upon the receiving the data, decrypts it using $K_{MCH(i)}$ and extracts the data.

For example consider the network architecture given in figure-1. Initially, the multicast source S distributes unique key $K_{sch(i)}$ with cluster heads CH3, CH17 and CH20. When S wants to transmit the data packet to node 2, it first encrypts the message using $K_{SCH(3)}$ and forwards it to CH3. CH3 upon receiving the message decrypts it using the $K_{SCH(3)}$ and extracts the data. CH3 then encrypts the data using $K_{MCH(2)}$ and delivers the data packets to N2. N2 upon the receiving the data decrypts it using $K_{MCH(2)}$ and retrieves the data.

3.4 Mobility Management

Since, MANET encompass of mobile nodes, handling mobility is a challenging task. To resolve this issue, our approach makes use of roaming protocol and our keying scheme supports the mobility management.

To support mobility in the multicast communication, each node is provided with a mobility key (M_i), it can be obtained through the cluster head (CH_i). The M_i key is generated through OFC. Any node cannot receive additional information from the M_i. Our multicast mobility management technique is as follows,

Step-1
The mobile node encrypts the message using $K_{SCH(i)}$
Step-2
Simultaneously, it encrypts the message again by M_i and includes its neighbor list. This encrypted message content is forwarded to the nearer CH.

Step-3
The CH that receives encrypted message first decrypts its mobility key M_i. Then it creates a multicast packet based on its neighbor list. Here, the multicast packet is created using Prufer encoding algorithm. [18] The generated Prufer sequence is included in the multicast packet header and then the message packet is forwarded.

Step-4
While receiving the packet, the desired CH makes decision of forwarding and dropping packet. This decision is done with received Prufer sequence and Prufer decoding algorithm. Finally, the packet is forwarded to the desired destination.

Step-5
The destination decrypts the message using $K_{SCH(i)}$ and retrieves the information.

Using Prufer and one-way function chain, our technique reduces the overhead that generally occurs in key management process. In addition to security, mobility is also managed by our multi level key management technique.

4. SIMULATION RESULTS

4.1 Simulation Model and Parameters

We use NS2 [19] to simulate our proposed protocol. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In our simulation, 50 mobile nodes move in a 1000 meter x 1000 meter region for 100 seconds simulation time. All nodes have the same transmission range of 250 meters. In our simulation, the node speed is fixed as 5m/s. The simulated traffic is Constant Bit Rate (CBR).

Our simulation settings and parameters are summarized in table I.

Journal of Theoretical and Applied Information Technology
20th March 2013. Vol. 49 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1. Simulation Parameters

No. of Nodes	50
Area Size	1000 X 1000
Mac	802.11
Routing Protocol	MGKMT
Radio Range	250m
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	500 bytes
Mobility Model	Random Way Point
Speed	5m/s
No. of Receivers	5,10,15,20 and 25
Pause time	5 s
No. of Attackers	1,2,3,4 and 5
Initial Energy	3.3 J
Transmission Power	0.660
Receiving Power	0.395
Transmission Rate	250Kb.

4.2. Performance Metrics

We evaluate mainly the performance according to the following metrics.

Average Energy: It is the average energy consumption involved in the entire data transmission.

Average Packet Delivery Ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

Packet Drop: It is the number of packets dropped during the data transmission.

Resilience against Node Capture: Here we are going to calculate how a node capture affects the rest of network resilience. It is calculated by estimating the fraction of communications compromised between non compromised nodes by a capture of x-nodes.

We compare our Multi-Level Group Key Management Technique (MGKMT) with the hierarchical key management scheme HKM [9] scheme. The simulation results are presented in the next section.

A. Based on Attackers

Initially in our first experiment we vary the number of attackers as 1,2,3,4 and 5.

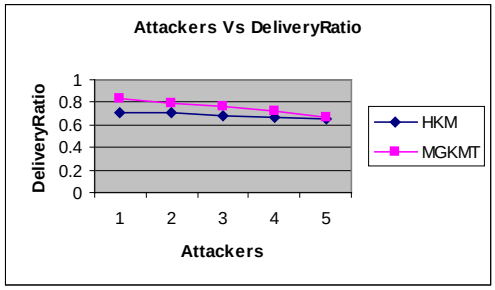

Figure 4: Attackers Vs Delivery Ratio

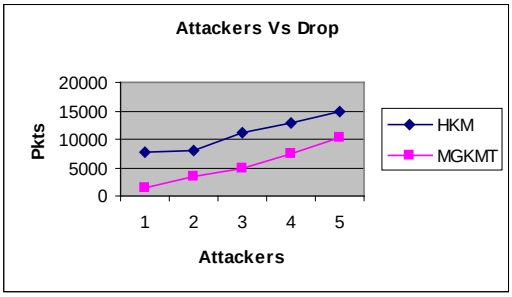

Figure 5: Attackers Vs Drop

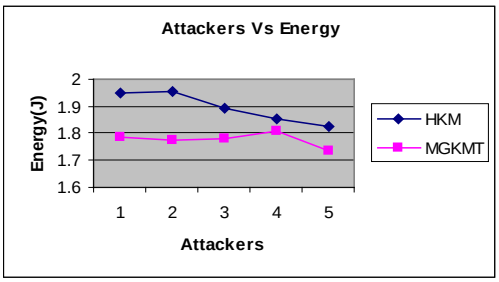

Figure 6: Attackers Vs Energy

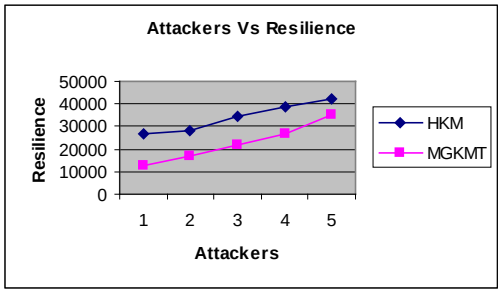

Figure 7: Attackers Vs Resilience

The average energy consumption of both the techniques is depicted in Figure 6. From the figure, we can see that the average energy consumption decreases, when the no. of attackers is increased. This is due to the reason that the percentage of correctly received data traffic reduces as the number of attackers is increased in the network. When compared to HKM, MGKMT has 6% less

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

energy consumption, because of the cluster based approach.

Figure 4 shows the packet delivery ratio of both the techniques. It is trivial that when more attackers are introduced, the packet drop is increased and hence the packet delivery ratio is decreased. But MGKMT has shown 9% performance improvement in packet delivery ratio, when compared to HKM. This is because of the fact that MGKMT uses the success ratio of both data and control packets which mitigates the effect the attackers.

From figure 7, we can see that the resilience of our proposed MGKMT is 36% less than the existing HKM technique.

B. Based on Receivers

In our second experiment we vary the number of receivers as 5,10,15,20 and 25, keeping the total attackers as 5.

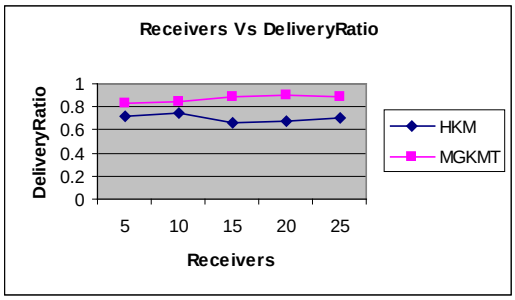

Figure 8: Receivers Vs Delivery Ratio

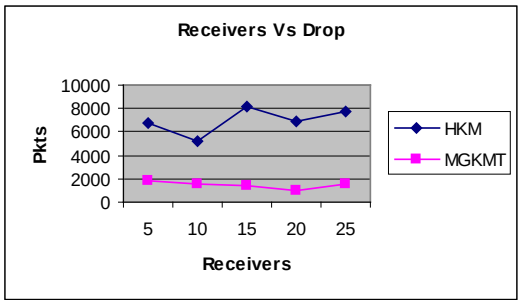

Figure 9: Receivers Vs Drop

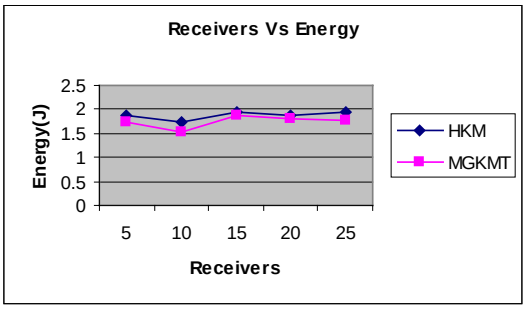

Figure 10: Receivers Vs Energy

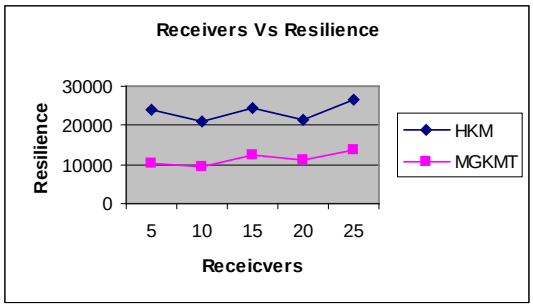

Figure 11: Receivers Vs Resilience

Figure 8 shows the packet delivery ratio of both the techniques. When the number of receivers is less than 15, the effect of 5 attackers is high, so that the packet drop is more and delivery ratio is less. But when the number of receivers is more than 15, the packet delivery ratio becomes constant. We can see that the packet delivery ratio of our proposed MGKMT is 18% higher than the existing HKM protocol.

The average energy consumption of both the techniques is depicted in Figure 10. From the figure, it can be seen that the energy consumption of MGKMT is 6.8% lower than the existing HKM protocol.

From figure 11, we can see that the resilience of our proposed MGKMT is 51% less than the existing HKM technique.

5. CONCLUSION

In this paper, we have proposed a multi level group key management technique for multicast security in MANET. Our technique works in a hierarchical model such that cluster heads are prioritized over cluster members. Initially, after the nodes are deployed in the network, node with high bandwidth and residual energy is elected as a cluster head. Once the cluster is formed, each cluster head (CH_i) generates a set of keys for its cluster members. Keys are generated using one-way function chain. The generated keys are distributed to the cluster members using shuffle algorithm. Apart from this secure transmission, our technique has considered the issue of mobility of nodes. The mobility management is achieved by means of Prufer algorithm. By simulation results, we have proved the proficiency of our proposed technique. Our secure key management technique incurs low energy consumption and significantly increases the packet delivery ratio of the network.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCES

[1] Fujian Qin, "QoS Topology Control with Energy Efficiency for MANET", *Journal of Convergence Information Technology*, 2011

[2] Jun-Zhao Sun, "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing", *IEEE International Conference on Info-tech and Info-net*, pp-316-321, 2001.

[3] Luo Junhai, Xue Liu and Ye Danxia, "Research on multicast routing protocols for mobile ad-hoc networks", *ELSEVIER Computer Networks*, pp- 988–997, 2008

[4] R. Kalaidasan, Mrs. V.Hemamalini and Anoop K Babu, "SORB: Secure On Demand Resilient to Byzantine Multicast Routing in Multihop Wireless Networks",

[5] Carlos de Morais Cordeiro, Hrishikesh Gossain and Dharma P. Agrawal, "Multicast over Wireless Mobile Ad Hoc Networks: Present and Future Directions", *IEEE Network*, pp- 52 – 59, 2003.

[6] P.Deepalakshmi and Dr.S.Radhakrishnan, "An Ant Colony Based Multi Objective Approach to Source-Initiated QoS Multicasting Method for Ad Hoc Networks", *International Journal of Advances in Soft Computing and Its Applications. (IJASCA)*, 2011

[7] N.Shanthi, Dr.L.Ganesan , And Dr.K.Ramar, "Study of Different Attacks on Multicast Mobile Ad Hoc Network", *Journal of Theoretical and Applied Information Technology*, 2009.

[8] Hoang Lan Nguyen and Uyen Trang Nguyen," A study of different types of attacks on multicast in mobile ad hoc networks", *ELSEVIER Ad Hoc Networks*, pp- 32–46, 2008.

[9] Nen-Chung Wang and Shian-Zhang Fang," A hierarchical key management scheme for secure group communications in mobile ad hoc networks", *The Journal of Systems and Software* 80(2007).

[10] Pavithira Loganathan and T. Purushothaman," An Energy Efficient Topology Aware Key Management Scheme for Multicasting in Ad-hoc Networks", *International Journal of Wisdom Based Computing*, Vol. 1 (3), December 2011

[11] Dijiang Huang and Deep Medhi," A secure group key management scheme for hierarchical mobile ad hoc networks", *Ad Hoc Networks* 6,560-577 (2008).

[12] R. Vennila and V. Duraisamy, "QoS Based Clustering Technique for Multicast Security in MANET", *European Journal of Scientific Research* ISSN 1450-216X Vol.81 No.1, pp.33-46, 2012

[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] Hua-Yi Lin and Tzu-Chiang Chiang," Efficient Key Agreements in Dynamic Multicast Height Balanced Tree for secure Multicast Communications in Ad Hoc Networks", *EURASIP Journal on Wireless Communications and Networking* Volume 2011, Article ID 382701, 15 pages.

[15] Attila A.Yavuz, Fatih Alag¨Oz and Emin Anarim," A new multi-tier adaptive military MANET security protocol using hybrid cryptography and signcryption", *Turk J Elec Eng & Comp Science*, Vol.18, No.1, 2010

[16] N. Vimala, B. Jayaram and Dr. R. Balasubramanian," An Efficient Rekeying Function Protocol with Multicast Key Distribution for Group Key Management in MANETs", *International Journal of Computer Applications* (0975 – 8887) Volume 19– No.2, April 2011.

[17] Bogdan Groza and Toma-Leonida Dragomir, "On the use of one-way chain based authentication protocols in secure control systems", *IEEE Second International Conference on Availability, Reliability and Security*, (ARES 2007), 2007

[18] C. Vanniarajan and Kamala Krithivasan, "Network (Tree) Topology Inference Based on Prüfer Sequence", *IEEE National Conference on Communications (NCC)*, pp-1-5, 2010

[19] Network Simulator: http:/// www.isi.edu/nsnam/ns