# Energy Efficient Security Framework and Mitigation of Black Hole Attack for Mobile Ad- Hoc Networks

Muthumayil. K
PSNA College of Engg. & Tech.,Dindigul,
Tamilnadu, India

Buvana. M
PSNA College of Engg.& Tech.,Dindigul,
Tamilnadu, India

***Abstract*—In mobile ad hoc networks, the security is the main constraint in message transmission. For secure group based message transmission, we must share the key among users so that we can make the transmission as secure. In this paper, we develop a security framework KAP that consists of two protocols namely, Subgroup Key Generation (SKG) and Group Key Generation (GKG) based on ECDH for subgroups and outer groups respectively. These subgroup keys and group keys should be changed when there are membership changes (such as when the current member leaves or the new member joins). Gateway member is selected for each group. By introducing group-based approach, messages and key updates will be limited within subgroup and outer group. Thus computation load is distributed to many mobile ad hoc nodes. Both theoretical and practical results show that this group key agreement protocol performs better in terms of memory storage, energy consumption, and delay.**

***Keywords—Mobile ad hoc network, Group key agreement, ECDH, Energy consumption, Delay***

## I. INTRODUCTION

Wireless networks are growing rapidly in last few years. In wireless networks, there are two classifications: Infrastructure-based wireless networks and Infrastructure less or ad-hoc wireless networks. Most wireless networks deployed today's life are IEEE 802.11 Wireless LANs. So there is a pre-established wired infrastructure for wireless LANs to connect various access points. But there are no wired connections in wireless ad hoc networks. Since the nodes are mobile nodes and there are no such pre-existing infrastructure. Nodes with wireless capability form an ad-hoc network in real time. In ad-hoc network, the mobile nodes are working as a normal mobile node and as well as routers which are forwarding the packets from one mobile node and another mobile node. Ad-hoc network is ideal for battlefield or rescuer areas where fixed infrastructure is very hard to deploy.

A mobile ad-hoc network is a collection of autonomous nodes that communicate with each other. Ad-hoc network needs of security mechanisms for secure communication. Providing security for ad-hoc mobile nodes is a very difficult task because of they all are mobile nodes without any infrastructure. Since there are high mobility among mobile nodes, we can't implement any security mechanism without a central node which is having capability to store the key pairs of all mobile nodes. Suppose the central node is moving frequently, then all key pairs of mobile nodes will be destroyed. Mobile nodes form an ad-hoc group for secure communication. In traditional wireless networks, a key distributed system is available as a third party that acts as an intermediate node between nodes of the network. Ad-hoc networks are not generally having a trusted third party. In group key agreement, multiple nodes form an group and generate a common secret key to be used to exchange information securely. A group member can leave or a new group member can join in the existing group. At that time, the group key agreement protocol needs to address the security issues related to the membership changes due to node mobility. In group key agreement protocol, all nodes within the group selects a group key [1] – [6] for secure transmission. The membership change requires frequent changes of group key.

There are many group key agreement protocols [7], [8], [9for providing security. These protocols are discussing about providing security for decentralized networks. In MANETs, there is no such central authority to provide security. In [1], the author discussed about how elliptic curve cryptography [ 10], [11]secure group communication. In [2], the gateway member is elected based on the highest power of node. But choosing the highest power node poses new problems in MANETs. In [7], the authenticated protocol was designed using the elliptic curve cryptography. But this is also vulnerable to some attacks. Our aim to design a new security protocol for MANETs using elliptic curve cryptography based on diffie-hellman key exchange. Before providing security, the gateway member should be elected based on the stability and power of the node. For power, we use to have transmitter energy and receiving energy.

We propose an efficient group key agreement protocol in ad-hoc network. In large and high mobility ad-hoc networks, it is not possible to use a single group key for the entire network because of cost of computation in rekeying. So we divide the group into many subgroups and each subgroup has its own subgroup key which is shared by all members of that subgroup. In each subgroup, one node is elected as a gateway node which is the controller among subgroups. Gateway node is elected based on the stability value of the node and power level of the node. Each gateway node in various subgroups forms an outer group and generates a outer group key.

## II. RELATED WORK

Krishnan Kumar et al [14] addressed an interesting security problem in wireless ad hoc networks: the Dynamic Group Key Agreement key establishment. They proposed a novel, secure, scalable and efficient Region-Based Group Key Agreement protocol (RBGKA) for ad-hoc networks. This was implemented by a two-level structure and a new scheme of group key update. The idea is to divide the group into subgroups, each maintaining its subgroup keys using Group Diffie-Hellman(GDH) Protocol and links with other subgroups in a Tree structure using Tree-based Group Diffie-Hellman (TGDH)protocol. K. Kaabneh and H. Al-Bdour [15] proposed a modified protocol for elliptic curve key exchange based on elliptic curve over rings, assuming that only the curve *E* and *Fq* are public, keeping the base point *P* secret, which make attacking the cryptosystem harder by the eavesdropper. Also they provided imbedded authentication, so their protocol does not suffer from the man in the middle attack. They prove that their protocol meets the following desirable security attributes. Known-Key Security, the protocol provides known key security. Each run of the protocol between two entities A and B should produce a unique session key.

Sergio Marti et al[16]proposed categorizing nodes based upon their dynamically measured behavior. They used a watchdog that identifies misbehaving nodes and a path rater that helps routing protocols avoid these nodes. Through simulation they assessed watchdog and path rater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection. When used together in a network with moderate mobility, the two techniques increase throughput by 17% in the presence of 40% misbehaving nodes, while increasing the percentage of overhead transmissions from the standard routing protocol's 9% to 17%. In [17], Rashid Hafeez Khokhar et al discussed the current security issues in MANET are investigated. Particularly, they have examined different routing attacks, such as flooding, black hole, link spoofing, wormhole, and colluding misrelay attacks, as well as existing solutions to protect MANET protocols. They have discussed current routing attacks and countermeasures against MANET protocols.

Debdutta Barman Roy et al [18] have discussed about the very severe type of attack called, wormhole attack. A particularly devastating attack is the wormhole attack, where a malicious node records control traffic at one location and tunnels it to another compromised node, possibly far away, which replays it locally. Routing security in ad hoc networks is often equated with strong and feasible node authentication and lightweight cryptography. Unfortunately, the wormhole attack can hardly be defeated by crypto graphical measures, as wormhole attackers do not create separate packets.

## III. PROPOSED SCHEME

### *A.. Motivation*

In mobile ad-hoc networks, the security is main concern in achieving the efficient and deployable network for military and rescuer areas. In security, there are three mechanisms to be maintained: Confidentiality, Authentication and Non-repudiation. Confidentiality maintains that the particular message is to be received by the authorized receiver. Authentication assures that the particular message is being sent by a authorized sender. Non-Repudiation assures that any sender or receiver could not able to deny the previous transactions (Sender cannot deny that the previous message had not been sent by me or receiver cannot deny that the previous message had been received by me). If any security algorithm provides these three security mechanisms, it will be a good and deployable security algorithm. But providing these mechanisms in ad-hoc networks is difficult since there are no such infrastructures. All these mechanisms need a central authority to store the key pairs of the mobile nodes. For example, in a military environment any one mobile node can be selected as a central node to which all other mobile nodes send their key pairs. In these networks, the nodes other than the central node have limited power and low stability.

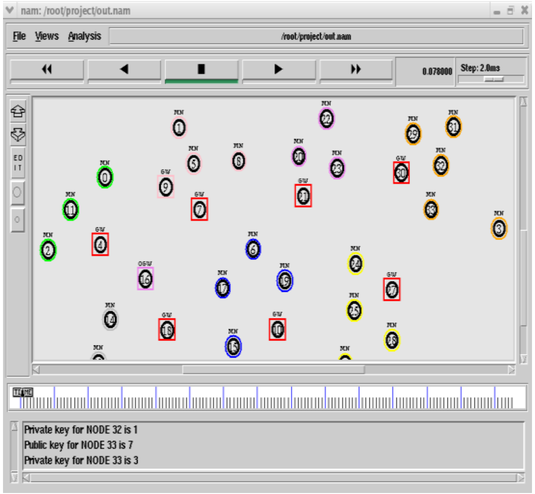
### *B. System model*

*a) Gateway member(GM)*

Among many nodes in subgroup, only one node is selected as a gateway member (GM) node. The criteria for the selection of gateway member node selection is: number of beacons transmitted and received by the node. If any node receives beacon signals more than the value of Received Beacon Threshold ($RB_{th}$), we assure that the node is a high stability node and it is selected as a *GM* of that group. Here we use transmitted beacons for computing remaining lifetime of the node. If any node transmits beacons below the value Transmitted Beacon Threshold ($TB_{th}$) , then that node is selected as a gateway member node as shown in figure 1. For our algorithm, if any one node satisfies both $RB_{th}$*and* $TB_{th}$, that node is selected as a GM.

```
    1. Network formation
    2. Subgroup formation
       S = N / j < 100
       Where N – No. of Nodes,
       j-- No. of subgroups needed.
 3.   Select GM
       If (RBeacon [Mi] ≥ $RB_{th}$)
   GM =  S [Mi]
Where   S [Mi]  = $i^{th}$ member of
the  subgroup S.
    4. Find the $PK_i$, $PU_i$ for each S [Mi]
    5. If  a  new node 'i' enters into
the subgroup S, findanew GM.
    6. Then go to step 3.
    7. For ( C = 0; ≤ j; C++ )
           Copy of the $GM_c$ to Outer
       Group.
    8.  Find the Outer GM by computing
          $RGM_{Beacon}$.
```

Algorithm 1: Finding Gateway Members



```
Private key for NODE 32 is 1
Public key for NODE 33 is 7
Private key for NODE 33 is 3
```

Figure 1: Simulation of Gateway and Outer Gateway Members

*b) Outer Gateway member*

Among many nodes in outer group, only one node is selected as a outer gateway member node. The criteria for the selection of outer gateway member node selection is: number of beacons received and transmitted by the node. If any node receives Beacon signals more than the value $RB_{th}$and transmits beacons below the value $TB_{th}$,then that node is selected as a outer gateway member.

- *Number of beacon signals received* $\geq RB_{th}$
- *Number of beacon signals transmitted* $\leq TB_{th}$

If these conditions are satisfied, the new gateway member (GM) and new outer gateway members are selected when at following situations:

```
   /* GM selected  */
   /* Key generation (SKG and GKG)*/
   1. user 'i' generates the private
      key PK_i
   2. user 'j' generates the private
      key PK_j
   3. users i& j calculate the public
      key.
              PU_i = PK_i * G.
              PU_j = PK_j *  G.
              G - Generated point in the
              elliptic curve.
 4.User i sends its public key PU_i  to
 user j
 5. User j computes subgroup key as
            SK_j =   PK_j * PU_i
 6. User j sends its public key PU_j  to
 user i
 7. User i computes subgroup key as
            SK_i =   PK_i * PU_j
  8. check SK_i = SK_j
  9. GM stores this key as SK_i,j
```

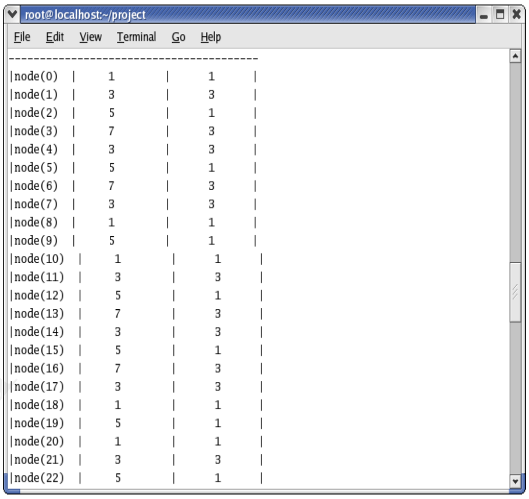
Algorithm 2 : key generation

*C. Key Agreement based on Power (KAP)*

KAP is a group key agreement protocol. It is used to generate the subgroup key for subgroups and outer group key for outer group (gateway members) control. It considers the movement of the mobile node inside the subgroup and mobility of gateway member in outer group. It consists of the following two protocols:

*i) Group Keys(SKG and GKG) Generation*

A gateway member is selected for each subgroup. All the nodes including the gateway member shares their partial keys to generate the subgroup key (SK). The gateway member acts as a controller for that subgroup. Hence all communications inside the subgroup and across the subgroups are taken through gateway member (GM) or controller.



```
----------------------------------------
|node(0)  |     1      |     1     |
|node(1)  |     3      |     3     |
|node(2)  |     5      |     1     |
|node(3)  |     7      |     3     |
|node(4)  |     3      |     3     |
|node(5)  |     5      |     1     |
|node(6)  |     7      |     3     |
|node(7)  |     3      |     3     |
|node(8)  |     1      |     1     |
|node(9)  |     5      |     1     |
|node(10)  |     1      |     1     |
|node(11)  |     3      |     3     |
|node(12)  |     5      |     1     |
|node(13)  |     7      |     3     |
|node(14)  |     3      |     3     |
|node(15)  |     5      |     1     |
|node(16)  |     7      |     3     |
|node(17)  |     3      |     3     |
|node(18)  |     1      |     1     |
|node(19)  |     5      |     1     |
|node(20)  |     1      |     1     |
|node(21)  |     3      |     3     |
|node(22)  |     5      |     1     |
```

Figure 2: Simulation of Private and Public keys

User *i* generates its private key $PK_i$ and calculates its public key $PU_i = PK_i * G$, where 'G' is a generated point in the elliptic curve. Likewise, user *i* generates its private key $PK_j$ and calculates the public key as $PU_j = PK_j * G$as shown in figure 2. Users *i* and *j* computes subgroup key as $SK_i$, $SK_j$ as per algorithm 2. If these two are keys are same, *SKi,j* is taken as subgroup key. Then the keys are exchanged successfully. Then gateway member *GM* stores this key in its storage. All the group members are further form a outer group and a outer gateway member is elected based on the principle of gateway member election as per algorithm1. From each subgroup, the gateway members are gathered and form as a outer group. Gateway members of each subgroup shares their partial keys to generate a outer group key as per same algorithm 2 . This $G_K$ is used for secure transmission of messages within gateway members those formed the outer group.

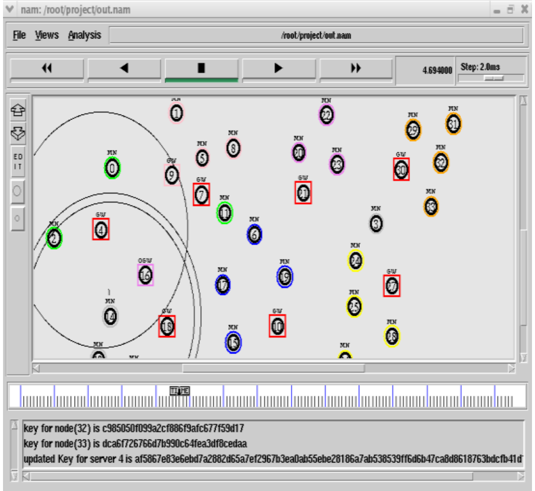
*D. Rekeying*

$S_K$ and $G_K$ are rekeyed when the following events happen:

*(1) When the previous outer gateway member(OGM) leaves*

*(2) When the current gateway member(GM) leaves*

*(3) When a standard member of the group leaves*



```
key for node(32) is c985050f099a2cf886f9afc677f59d17
key for node(33) is dca6f726766d7b990c64fea3df8cedaa
updated Key for server 4 is af5867e83e6ebd7a2882d65a7ef2967b3ea0ab55ebe28186a7ab538539ff6d6b47ca8d8618763bdcfb41d
```

Figure 3 : Simulation of Re-keying

*(4) When a new member wishes to join in the existing group*

In figure 3, we can see that re-keying is done for node 4, when the node 0 is added in the group as shown in algorithm 3. Also, any of the nodes in that group leaves, the re-keying is done as shown in algorithms 3and 4.Thus the new $S_K$ and $G_K$ are used as a key for further secure transmissions.

```
/*Rekeying : Member joins*/
n – new node is joining into S
    1. if new node 'n' enters in to
       the subgroup S.
    2. 'n' – generates its private
       key. $PK_n$& $PU_n$ = $PK_n$ x G.
    3. GM sends the public keys of i
       and j, group key of [i,j]
    4. 'n' uses the group key of
       [i,j] and compute $SK_{i,j,n}$ = PK $_n$
       x $SK_{i,j}$
    5. 'n' calculates the following
       public keys
$PU_{j,n}$ = $PK_n$* $PU_j$ and
$PU_{i,n}$ = $PK_n$ * $PU_i$
    6. user 'n' broadcasts these
       group keys to i and j
    7. j computes a new subgroup key
       $SK_{i,j,n}$ = $PK_j$ * $PU_{i,n}$
    8. i computes a new subgroup key
       $SK_{i,j,n}$ = $PK_i$ * $PU_{j,n}$
    9. check the new subgroup key of
       i,j and n is $SK_{i,j,n}$
```

```
/*Rekeying : Member & leaves*/
'j' leaves from S
/* when member 'j' leaves from the
subgroup */
   1.GM, 'i' changes its private key
$PK_i$, then Calculates new public
key $PU_i$ = $PK_i$* G
   2.'i' shares its public key with
user 'n'
   3.n computes the subgroup key as
$SK_n$ = $PK_n$ * $PU_i$
   4.i computes the subgroup key as
$SK_i$ = $PK_i$ * $PU_n$
5. check $SK_i$ = $SK_n$
6. Then GM 'i' stores this key as
$SK_{i,n}$
```

Algorithm 4:Re-keying while Node Moves

## IV. ATTACKS

Since there are no such infrastructure, like having access point and central coordinator in MANETs, the nodes are having no security among themselves. The traditional security algorithms cannot be used in MANETs because of high mobility and highly dynamic topology. In traditional networks, there are two types of attacks such as passive attack and active attack. Passive attacks are less harmful than active attack. The attackers are simply stealing the data but not modifying the information. But in active attacks, the attackers are compromising the data also modifying the information. Thus active attacks are very harmful than passive attacks. In this work,, we have taken the active attacks into our consideration. In MANETs, the active attacks are classified into different types namely, wormhole attack, black hole attack, rushing attack, jelly fish attack, denial of service attack and so on. In this paper, we have taken the black hole attack for our security analysis.

### *A. Black hole attack*

It is one of the types of active attacks in MANETs. A wormhole attack is a particularly severe attack on MANET routing where an attacker takes part in a network and captures the packet. These attackers then record the wireless data they overhear, forward it to each other, and copy or replay the packets at the other end of the network. Replaying valid network messages at improper places, black hole attackers can make far apart nodes believe that they have a route to the destination.

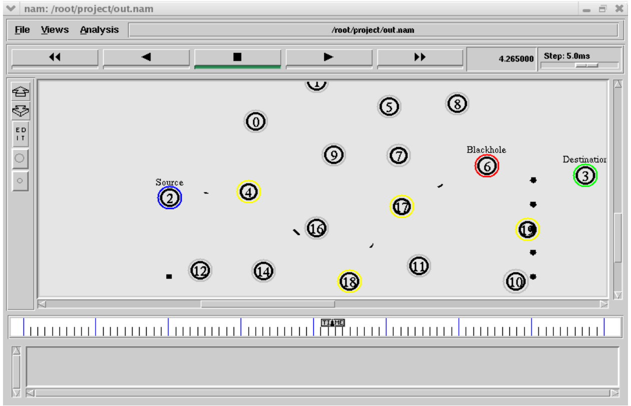


Figure 4: Black hole node captures the packets and replies

In figure 4, the node 6 is detected as a black hole node. Then node 6 captures the packets from source node 2. node 6 sends the route reply back to the source node 2 along multi-hops that node 6 have the path to the particular destination 3. Normally the neighbor nodes of the black hole node 6 do not know about the presence of attack. We use remaining energy and transmission range of the node to detect the black hole attack.

### B. *Security Analysis of Black hole Attack*

In black hole attack, there are some possibilities of having compromised nodes very nearer to the destination. The destination will not know about the attacker node. This type of attack can be identified by using transmission range among the nodes. So each node should have a routing table, in which the remaining energy and transmission range [13] of the nearby nodes are stored and used whenever it is needed. For example, the attacker node N1 is very nearer to the nodes A and C respectively. So both nodes A and C should know about the remaining energy and transmission range of the previously nearby nodes and therefore easily find out the new nodes that are attackers. But it is difficult to know about how and when the attacker node comes very closer to the source and destination nodes in ad hoc networks since there are high mobility among the nodes.

#### *i) By using the remaining energy*

As we know that there is power dissipation in mobile nodes whenever there is transmission of any packet or signal, reception of any packet or signal and also in idle state. After forming the group into subgroups in this work, the member of the group can find the gateway member that will be full in-charge of that particular group. For finding the gateway member, we are using the received beacons. Since every node is sending the beacons at regular intervals, there is power consumption at nodes always. By sending the beacons, one can lose the energy. By receiving the beacons, one can lose the energy. Likewise, every node is losing their energies in any of these forms such as transmission, reception and idle. After every mode of above said communication takes place, the node will find the remaining energy from the initial energy and consumed energy. These energy levels are stored and sent to their neighbor nodes. The neighbor nodes are storing this energy level and it will be used for future use. To know about the node's remaining energy, we have to calculate the bit rate transmission and energy which is spent upon transmission and reception of any messages.

The bit energy is written as

$$E_b = P_r / R_b \qquad (1)$$

Where, $R_b$ is the bit rate

The receiver sensitivity is defined as the minimum received power ($P_{Rmin}$) necessary for a signal to be correctly detected. The receiver strength is the only one parameter which decides the correct reception of signals. The sender uses this $P_{Rmin}$ for further transmissions.

The total amount of energy consumed per transmitted packet is written as

$$E_t = P_T * L / R_b \qquad (2)$$

Where,$E_t$is the transmitted energy, L is the packet length

The total amount of energy consumed per received packet is written as

$$E_r = P_{Rmin} * L / R_b \qquad (3)$$

then calculates the residual energy $E_{res}$ using the following

parameters:

$E_I$ – Initial energy taken by the node
$E_t$ – Energy consumed in transmitting packets
$E_r$ – Energy consumed in receiving packets
$E_i$ – Energy consumption in idle state.

$$E_{res} = E_T - (E_t + E_r + E_i) \qquad (4)$$

#### *ii) By using the transmission range*

Each node has to find out the nearest neighbor based on the principle of geographically nearest node using the transmission range (distance between sender and receiver). To find the geographically nearest node, we have to calculate the transmission range. Transmission range $T_R$ is given by

$$T_R = \frac{G_T G_R P_T (H_T H_R)^2}{P_{R\min}} \qquad (5)$$

Where $P_T$ is the transmission power, $G_T$and $G_R$ are gains of transmitter and receiver respectively, $H_T$ and $H_R$ are the heights of transmitter and receiver respectively and $P_{Rmin}$ is the minimum receiving power of the receiver. In this technique, the transmission range of the nodes is appended with the messages which are transmitted among other nodes.

### C. *Mitigation of Black hole attack*

In this work, we have designed a malicious node detection technique in elliptic curve diffie-hellman key agreement protocol. For mitigating the black hole attack, the users are measuring their remaining energy and transmission range with the neighbors. This information is delivered to their neighbors.

Those neighbors are storing the information in it's table. If any node is compromising, it will be detected at receiver by checking remaining energy and transmission range of that particular node.

For avoiding the black hole attack in subgroup key generation (Algorithm 5), re-keying when a member joins and a member leaves, the user *i* sends its public key along with residual energy of it, $E_{res}$ and its transmission range, $T_{R.}$ as in algorithms 5 and 6. So neighbor nodes store this information user *i* in their storage. In future, if any wormhole attackers are moving inside the group, the neighbor nodes can identify the attacker nodes by using the remaining energy and transmission energy of that particular node. Since all the nodes are moving inside the environment, we cannot expect the malicious nodes transmission range with their neighbor nodes which are non-compromised nodes. So we can have the transmission range threshold $T_{Rth.}$ If the transmission range value increases for a node, then that particular node is noticed as a attacker node in its neighboring node table. If any node receiving the any other node's transmission range is lower than the threshold value, immediately that node is noticed as a attacker node and no message is passed along that node. The algorithm 5 explains the prevention of black hole attack while key generation and re-keying

## V. PERFORMANCE ANALYSIS

In our scheme, there are two protocols namely, SKG and GKG. These two protocols develop two keys which are used within the subgroup and in the outer group respectively. These two protocols are working after finding the gateway member or controller for the subgroup and for outer group. Using the power of the mobile node, the stability can be calculated in this protocol. This algorithm is designed for the low power mobile ad hoc nodes which require smaller key sizes and smaller memory requirement.

As per the memory to store the keys at member nodes as well as in gateway members, the ECC makes the process as easy as possible. Since the key sizes are small in ECC, the storage capacity at nodes are very small than other symmetric key types like AES. In our group key agreement protocol, the keys are stored by GM for that group only. But in tree-based approaches, each node has to maintain the keys of its leaf nodes and so on. Our approach consumes very low memory storage cost than tree based approaches.

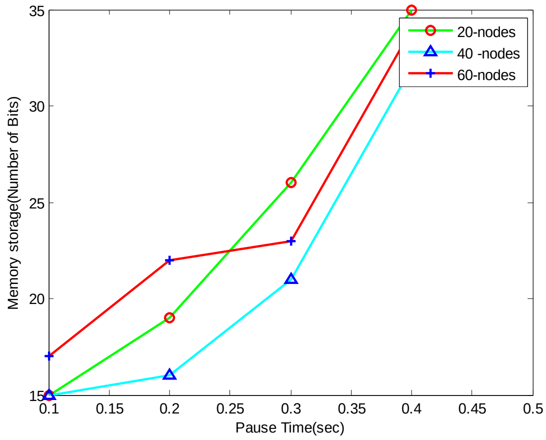


Figure 5: Variation in memory storage with pause time

The memory storage gets affected when the mobility is high, that is depicted in figure 8. If the number of mobile nodes is high, the movement of the nodes is also high. When the number of nodes is 20, the memory storage peaks to high suddenly and falls down and then it peaks to high. This is due to high and sudden movement of the nodes. So the GM has to store many temporary keys since the movement of the nodes. When the number of nodes is 60, the memory storage is good at starting but it gets lower performance finally as 20 nodes and 40 nodes.

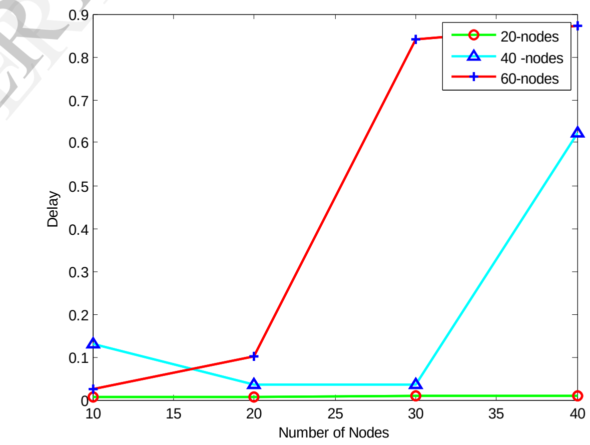


Figure 6: Variation in delay with number of nodes

The delay that is depicted in figure 8 and figure 9, defined as diference between the time at which the packets are sent and time at which the packets are received. Our simulation shows that the delay is very low when the number of nodes is less that is 20. But the delay becomes high when the number of nodes is 40 and 60. The delay is high when the movement of nodes is very high in the case of 60 nodes. But when the number of nodes is 40 and mobility is high, the delay peaks to high from its starting point finally it gets down since there are no movement of the nodes. The delay for 20 nodes is very low however there is little movement of nodes.

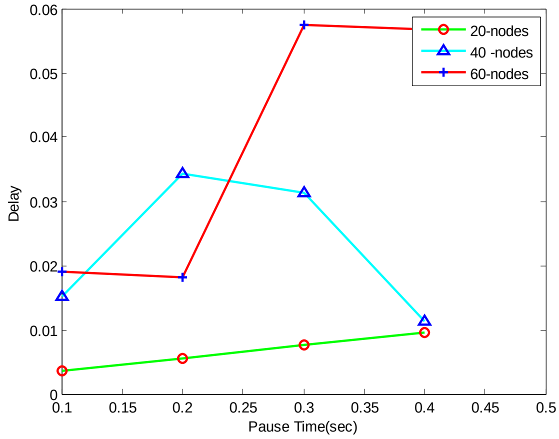


Figure 7: Variation in Delay with pause time

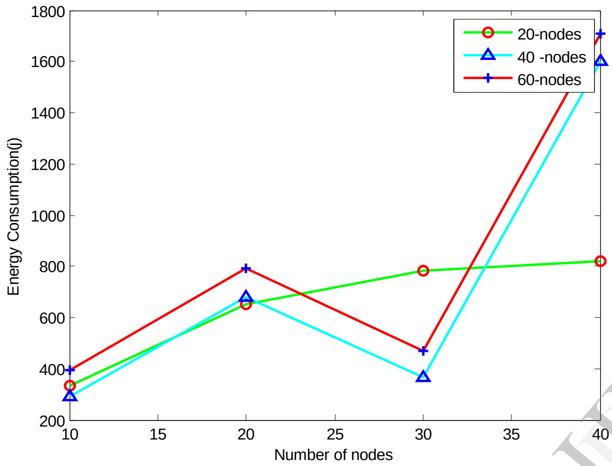


Figure 8: Energy consumption Vs Number of nodes

The energy consumed by the cluster nodes and gateway member is very high for the number of nodes 40 and 60 is depicted in both figure 10 and figure 11. Here, the energy consumption is very high due to the count of beacons and calculation of transmitted and received beacons by every node.

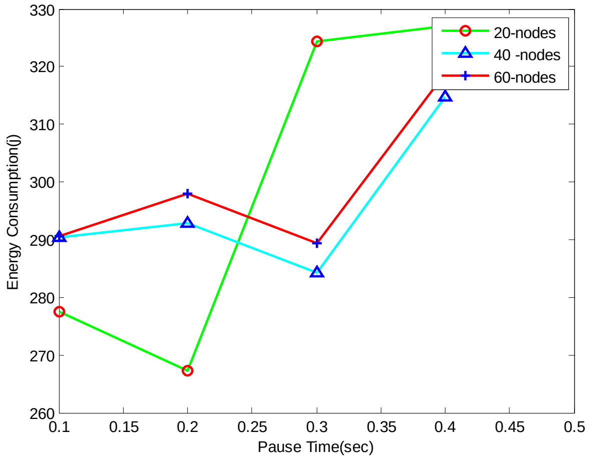


Figure 9. Energy consumption vs Pause time

When the mobility of the nodes is low for 20 nodes, the energy consumption is high because of very less computation of beacons by node movement. But for the 40 nd 60 nodes, the energy consumption is high because of node mobility. The delayed messges are comsuming more energy since there is high movement among the nodes. Also the re-keying procedure is comsuming more power due to sudden displacement of mobile nodes.

## VI. CONCLUSIONS

Our scheme called KAP provides two algorithms namely SKG and GKG. Based on the calculated number of beacons that are received by a node and transmitted by a node, we can select a best gateway member than previous designed protocols. Also the subgroup and group keys should be rekeyed whenever the membership changes (a node is joining or leaving). Our scheme provides better security for the black hole attack prevention in terms of remaining energy and transmission range of the nodes and quality of service parameters are such as memory storage, energy consumption and delay getting improved.

## REFERENCES

[1] Wang.Y, B. Ramamurthy and. ZouX. K, 2006:"The Performance of Elliptic Curve Based Group Diffie-Hellman Protocols for Secure Group Communicationover Ad Hoc Networks".,doi :10.1109/ICC.2006.255104

[2] Kumar.K, NafeesaBegum.J, Sumathy.V.2010, A Novel Approach towards Cost Effective Region-Based Group Key Agreement Protocol for Secure Group Communication.International Journal of Computer Science and Information Security, Vol. 8, No. 2 pp 65-74

[3] NachikethPotlapally.R, Srivaths Ravi, AnandRaghunathan and NirajK.Jha.2006: "A study of the Energy Consumption Characteristics of cryptographicalgorithms and security protocols". IEEE Transactions on Mobile Computing, Vol. 5, No 2,pp. 128- 148

[4] KavithaAmmayappan,AshutoshSaxena and AtulNegi.2006:"Mutual Authentication and Key Agreement based on Elliptic Curve Cryptography for GSM". doi:10.1109/ADCOM.2006.4289879

[5] WEI Chu-yuan, 2010 "A Hybrid Group Key Management Architecture for Heterogeneous MANET",, doi : 10.1109/NSWCTC.2010.256

[6] HishamDahshan and James Irvine, 2010. "An Elliptic Curve Distributed Key Management for Mobile Ad Hoc Networks". .doi: 10.1109/VETECS.2010.5494203

[7] Rajeswari.P.G.,Thilagavathi.K.2009, "An Efficient Authentication Protocol Based on Elliptic Curve Cryptography for Mobile Networks".IJCSNS International Journal of Computer Science and Network Security, Vol.9 No.2, pp 176-185

[8] Nils Gura, Sheueling Chang Shantz, Hans Eberle, Sumit Gupta, Vipul Gupta, Daniel Finchelstein, EdouardGoupy, and Douglas Stebila. 2003: "An End-to-End Systems Approach to Elliptic Curve Cryptography". doi:10.1.1.92.5128

[9] Kaabneh.K and Al-Bdour.H.2005: "Key Exchange Protocol in Elliptic Curve Cryptography with No Public Point". American Journal of Applied Sciences, Vol 2, Issue 8, pp1232-1235

[10] Vijayalakshmi.V andPalanivelu .T.G. 2007, "SecureAntnet Routing Algorithm for Scalable Adhoc Networks Using Elliptic Curve Cryptography".Journal of Computer Science, Vol3, Issue 12, pp 939-943

[11] NafeesaBegum.J, Kumar.K, Sumathy.V. 2011, "Multilevel Access Control in aMANET for a Defense Messaging system using Elliptic curveCryptography".International Journal of Computer Science & Security (IJCSS), Volume 4, Issue 2, pp 208-225

[12] Muthumayil,K, Rajamani.V and Manikandan.S, Buvana.M, 2011, "A Novel Cross layered Energy based on-demand routing protocol for Mobile ad hoc networks". doi:10.1109/ICoAC.2011.6165188

[13] Muthumayil.K, Rajamani.V and Manikandan.S, Buvana.M, 2011, "A Group Key Agreement Protocol based onstability and power using Elliptic curvecryptography". doi:10.1109/ICETECT.2011.5760274

[14] Krishnan Kumar, J. Nafeesa Begum, V. Sumathy, 2010, "A Novel Approach towards Cost Effective Region-Based Group Key Agreement Protocol for Ad Hoc Networks Using Elliptic Curve Cryptography" doi:10.4236/ijcns.2010.34047

[15] Kaabneh.K and Al-Bdour.H.2005, " Key Exchange Protocol in Elliptic Curve Cryptography with No Public Point". American Journal of Applied Sciences Vol 2,Issue 8,pp1232-1235

[16] Sergio Marti, Giuli.T.J, Kelvin Lai, Mary Baker 2010, "Mitigating routing misbehavior in mobile ad hoc networks". doi:10.1145/345910.345955

[17] Rashid HafeezKhokhar, MdAsriNgadi, Satria Mandala.2009, "A Review of Current Routing Attacks in Mobile ad hoc networks".International Journal of Computer Science and Security, volume 2 Issue 3,pp 18-29

[18] Debdutta Barman Roy, RituparnaChaki, NabenduChaki. 2009, "A NewCluster-based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Networks". International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, pp 44-52.