Middle-East Journal of Scientific Research 22 (1): 91-98, 2014
ISSN 1990-9233
© IDOSI Publications, 2014
DOI: 10.5829/idosi.mejsr.2014.22.01.21828

A Secure Hashed Variable Bit Rate Source Routing Protocol and Mitigation of Wormhole Attack for Manets

[1]R. Rajamohamed and [2]V. Rajamani

[1]Department of ECE St Peter's University Chennai, India
[2]Veltech Multitech Dr. Rangarajan Dr. Sagunthala Engg. College Vel Tech Avadi, Chennai, India

Abstract: In Mobile ad hoc networks, security is one among the many challenges to be taken care of Passive attacks and active attacks are the common types of attacks in Mobile ad hoc networks of which active attacks are more harmful than passive attacks, as there is no central coordination in MANETs. Examples of active attacks are: Worm hole attack, Black hole attack and Distributed Denial of Service (DDoS) attack and etc., In this paper, Hashed VBSR is taken into consideration. In Hashed VBSR clusters are formed based on the distance from all the nodes to a central node. Then the one time keys are managed among the user inside the cluster. Gateway members are playing the main role in group formation and preventing these attacks. In this Secure Hashed VBSR proposed work, the wormhole attack is discussed and security is analyzed.

Key words: MANET · Wormhole · Block hole · Hashed VBSR.

INTRODUCTION

As we increasingly rely on information systems, computers and networks, to support critical operations in telecommunication, banking, electronic commerce, defense and other systems, intrusions present serious obstacles and threats on the deployment of various computing systems and networks. Undoubtedly, if the next generation of network technology is to operate beyond the levels of current networks, security is one of the main concerns and issues to be addressed. Up to now, various solutions for data protection during transmission have been proposed and applied in a hierarchical manner. For example, at the application layer the information may be protected by authentication protocols, digital signatures and encryption techniques [1]. There are also many techniques that can be used to intercept information during data transfer, to generate and inject known and novel attacks and anomalies in the network.In wireless networks, nodes have limited resources and battery and forwarding data is resource consuming. Thus, a node may not be spending its resources to forward data for other nodes. Some of other protocols assume that nodes are malicious and they will destroy the network and damage other nodes as in Ariadne [2] and SAR [3]. Malicious nodes falsify packets of other nodes. With these selfish and malicious behavior the wireless network would not work properly. Attacks on the Internet can lead to enormous destruction [4], since different infrastructure components of Internet have implicit or explicit relationships with each other. Furthermore the performances of various classes of traffic in Internet are strongly correlated and therefore the performance degradation in one class due to an attack, may impact negatively the performances of other services as well, therefore leading to several anomalies. There are several types of attacks in the Internet that may range from Wormhole attack, Black hole attack and Distributed Denial of Service (D DoS) attack and etc., [5]. These attacks may affect a single user or the prformance of a large group of users or classes of service may get affected. In this paper, we mainly emphasize on the detection of attacks and/or intrusions that fall in the worm hole and black hole attacks since in general they present an impact on the performance of the whole network, or of a significant part of it. These attacks become extremely dangerous and very hard to prevent. Furthermore, in Ad hoc networks exists a strong motivation for non-participation in the routing system. Both the routing system and the forwarding of foreign packets consume a node's battery power, CPU time and bandwidth, which are restricted in mobile devices.

Corresponding Author: V. Rajamani, Department of ECE St Peter's University Chennai, India, Veltech Multitech Dr. Rangarajan Dr. Sagunthala Engg. College Vel Tech Avadi, Chennai, India.

Consequently, selfish nodes [6] may want to save their resources for own use. There are three main causes for a node not to work according to the common routing protocol: Selfish nodes try to save their own resources. Malicious nodes try to sabotage other nodes or even the whole network, or compromise security in some way. In this paper, we propose a new method to prevent the wormhole and black hole attacks. Section 2 explains the previous works that were carried out in the past years. Section 3 provides basic information about the attacks and types of attacks. Section 4 describes the wormhole attack proposed scheme which rectifies the problem and develop a new scheme to prevent the attacks. Section 5 describes about the simulation made on packet delivery ratio, throughput and routing overhead over misbehavior nodes.

Related Work: K.Muthumayil *et al* [6] addressed an interesting security problem in mobile ad hoc networks that is dynamic group key agreement for key establishment. All group members share a secure key to allow secure communication. When the existing group members leave the network or new members enter into the existing network this secure group key must be updated. They proposed a group key agreement protocol called Key Agreement protocol based on Stability and Power (KASP). Here the scheme is that larger groups are split into several smaller subgroups and each is assigned a subgroup key to manage the subgroup using Elliptic Curve Diffie-Hellman (ECDH) key agreement algorithm. In KASP, two protocols namely, Subgroup Key Generation (SKG) and Group Key Generation (GKG) based on ECDH for subgroups and outer groups are developed. When there are membership changes (such as when the current member leaves or the new member joins) the subgroup keys and group keys are changed. Krishnan Kumar *et al* [7] address an interesting security problem in wireless ad hoc networks: the Dynamic Group Key Agreement key establishment. A novel, safe, scalable and efficient Region-Based Group Key Agreement protocol (RBGKA) for ad-hoc networks was proposed. This was implemented by a two-level structure and a new scheme of group key update. The scheme divides each group into subgroups and assigns subgroup keys using Group Diffie-Hellman (GDH) Protocol and it is linked with other subgroups in a Tree structure using Tree-based Group Diffie-Hellman (TGDH) protocol. By introducing region-based approach, the messages and key updates will be restricted within a subgroup and outer group. Hence computational load is shared by many hosts. K. Kaabneh and H. Al-Bdour [8] 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. This keeps the base point *P* secret, thus making the attack on 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 proved 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. Although an adversary has learned some other session keys, he can't compute K, because he doesn't know private keys d. Perfect Forward Secrecy, it also possesses forward secrecy. Suppose that shared key is compromised. However, the secrecy of previous session keys established by honest entities is not affected, because in each time the two parties need to share a session key they select different points in the elliptic curve and different ephemeral key. It also prevents unknown key share making it difficult for the attacker to recognize the private key or the shared key. Sergio Marti *et al* [9] 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 parameters like packet throughput, percentage of overhead (routing) transmissions and the accuracy of malicious node detection. In a network with moderate mobility when this method is used the throughput increased by 17% in the presence of 40% misbehaving nodes and the percentage of overhead transmissions increased from the standard routing protocol's 9% to 17%. In [10], Rashid HafeezKhokhar *et al* discussed the current security issues in MANET which have been investigated. Particularly, they have examined different routing attacks, such as flooding, black hole, link spoofing, wormhole and colluding misrelay attacks and also other existing methods for secure communication using MANET protocols. They have discussed existing routing attacks and measures to reduce harmful nodes in MANET protocols. Some cryptography and key management techniques seem capable, but they are too expensive for resource constraint in MANET. But still trade-offs is needed between effectiveness and efficiency. Solutions work well in the presence of one attacker node, but are not effective in the presence of multiple attacker nodes. Special hardware such as a GPS or a modification to the existing protocol is required in some cases.Debdutta Barman Roy *et al* [11] have discussed about the very severe type of attack called, wormhole attack. Another dangerous attack is the wormhole attack, in which the attacker node records control traffic at one location and forwards it to another compromised node which is far away and this node replays it locally. Routing security in ad hoc networks requires strong and feasible node authentication and lightweight cryptography. But cryptographical measures are not that efficient on wormhole attack, as wormhole attackers do not create separate packets. Already existing packets are replayed on the network, which get ahead of the cryptographic checks. Existing methods use specialized hardware, such as directional antennas for wormhole detection. In this paper, they have presented a cluster based counter-measure for the wormhole attack that alleviates these drawbacks and efficiently mitigates the wormhole attack in MANET.Rutvij H. Jhaveri [12] *et al* have proposed a method to detect wormhole attack against AODV protocol. The work concentrates on finding some basic security concerns in MANET, functioning of wormhole attack and securing the well-known routing protocol Ad-hoc On Demand Distance Vector. Wormhole attack commonly involves two remote malicious nodes shown as X and Y. X and Y both are connected via a wormhole link and they target to attack the source node S. Wormhole attack is a real threat against AODV protocol in MANET. Therefore, reliable techniques for diagnosing and detection of wormhole attack become a necessity.

Attacks: Since there are no such infrastructure, like access point and central coordinator in MANETs, the nodes have 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 simply steal the data but they do not modify the information. But in active attacks, the attackers compromises the data also modify the information. Thus active attacks are more harmful than passive attacks. In this work, we have taken the active attack 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 wormhole attack for our security analysis. Ingeneral, there are two types of attacks in network security namely passive attack and active attack. Passive attacks are less harmful than active attack since they do not affect or modify the existing data. But active attack modifies the existing data. Since there is no central control entity in mobile ad hoc networks, the nodes have to keep themselves secure. The following are the popular types of active attacks in MANET:

- Wormhole attack
- Blackhole attack
- Rushing attack
- Sinkhole attack
- Sybil attack and so on.

There are two types of routing protocols in MANET namely proactive and reactive routing protocols. Both the protocols are affected by these active attacks. When we use proactive routing protocol such as DSDV and WRP, the nodes are periodically sending HELLO and BEACON signals to every other node in the network. When a source node S wants to send the data to destination D, it may send the data through some malicious node M. after getting the data, it will forward the data to D. In this time the destination D will not know about the presence of M and thinks that S and itself are direct neighbors. If D wants to send some data to S, D is unknowingly sending the data S through malicious node M.

On-demand routing protocols such AODV, DSR and etc., is also affected by the same way. That is, if a source node S wants to communicate with a destination node D, it will initiate to send route request packets. These RREQ packets are forwarded through malicious nodes unknowingly. So D will think that the packets come only from S. These type of wormholes are possible more often in mobile ad hoc networks. The malicious node can attack in MANET using different ways, such as sending fake messages several times, fake routing information and advertising fake links to disrupt routing operations[12].

Wormhole Attack: Wormhole attack is a silent and severe type of attack since it simply copies the packet at one location and replays them at different location or within the same network. So, in wormhole attack, there are two neighbor malicious nodes. They copy the packet at one location and replay the same packets without any changes in the content at different location or within the same network.For example, if a source node S wants to communicate with a destination node D, S will initiate the route request packets to its neighbors B and C. then both B and C forward the route request packets to their neighbors. But C doesn't know about the presence of such pair of malicious nodes M1 and M2. When M1 receives the packet, it forwards or tunnels the packet to its pair M2. Then M2 forwards the packet to E and E sends the packet to destination D. This time D will not about the malicious nodes M1 and M2. Also the route request packets are forwarded through multiple paths in on-demand routing protocols. In this scenario, the route request packets are sent through B also. B forwards the packet to F and F forwards the packet to destination D. But D ignores the second path that is via S-B-F-D only it accepts the path S-C-D. But the path S-C-D involves two malicious nodes. In future, D will select the path D-C-S to send the data to S.

Blackhole Attack: Blackhole attack is also an important and suspicious attack in mobile ad hoc networks. It sends fake or false routing information to the source node that it has fresh routing path from source to destination. In on-demand routing protocol, a source node S initiates the transmission by sending route request (RREQ) packets to its neighbors. The neighbor nodes forward the packets to their neighbors till the route request packets are sent to the destination. In blackhole attack, the attacker captures the route request packets and sends route reply (RREP) packets back to the source node S that it has the fresh route from S to destination D. Source node S discards the other route reply packets that are coming from other route. Once the attacker node sends route reply packet to S, S thinks that it is sending the data along that path to the destination. But the data is transmitted only to the attacker node. And the attacker node will choose whether to forward the data or discard the data.

Rushing Attack: Rushing attack is one of the most important types of Denial of Service (DoS) attack. It is against all currently reactive (on-demand) routing protocols in MANETs. An attacker can forward route request packets (RREQs) more quickly than legitimate nodes and thus increase the chance that routes which include the attacker will be discovered rather than other valid routes. After the attacker includes itself into the routes, it can launch different attacks such as dropping the packets that it receives, or modify the content of the packets.

Sinkhole Attack: In a sinkhole attack for ad hoc and sensor networks, the attacker tries to attract all traffic from a particular area through a compromised node. This creates a metaphorical sinkhole with the attacker at the center. Like black hole attacks in ad hoc networks, sinkhole attacks typically work by making a compromised node look particularly attractive to surrounding nodes with respect to the routing algorithm.

Sybil Attack: Sybil attack is a case in which the attacker presents multiple identities to other nodes in the network. It can considerably reduce the effectiveness of fault-tolerant distributed storage systems, routing algorithms, data aggregation, voting, fair resource allocation and so on.

In this work, we have wormhole attack is analyzed and security solution is given.

Worm Hole Attack: It is one of the types of active attacks in MANETs. A wormhole attack is a severe attack on MANET routing where two attackers are connected by a high-speed off-channel link and are placed at different ends of a network. These attacker nodes record the wireless data they overhear. Then they forward the data to each other and replay the packets at the other end of the network. Replaying important network messages at inappropriate places, wormhole attackers can make far apart nodes believe they are immediate neighbors and force all communications between affected nodes to go through them.

Security Analysis of Wormhole Attack: In wormhole attacks, there are some possibilities of having compromised nodes very nearer to the destination. At that time, the destinations do not know about the particular 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 of the nearby nodes are stored and used whenever it is needed. For example, the attacker nodes N1 and N2 are 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. There are two types of topologies. They are,

- Fixed topology
- Random topology

In fixed topology, the above said conditions are very easy to find the attacker because there are fixed nodes for longer time. But in random topology, we can't find the movement of the nodes since there are high mobility. For example, a node is in location *l1* at time *t1*. But the same node may or may not be in the same location, it may be in a new location *l2* at time *t2*. Also it is very easy to find the remaining energy of neighbor nodes since there are long lasting neighbor nodes but that is not the case in random topology. Thus random topology is taken into consideration.

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 is 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 use the received beacons. Since every node is sends 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 save the energy. Likewise, every node loses their energies in any of these forms such as transmissions, receptions and idle state. 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 store 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

$$E_b = P_r / R_b \tag{1}$$

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

$$E_t = P_T * L / R_b \tag{2}$$

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

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

$$E_r = P_{Rmin} * L / R_b \tag{3}$$

Then the residual energy E_{res} is calculated 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.

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

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

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

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 ranges of the nodes are appended with the messages which are transmitted among other nodes.

Mitigation of Wormhole Attack: In this work, we have designed a malicious node detection technique in elliptic curve diffie-hellman key agreement protocol. For mitigating the wormhole attack, the users measure their remaining energy and transmission range with the neighbors'. And this information is delivered to their neighbor. Those neighbors store the information in their 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 wormhole attack, the user *i*sends its public key [7] along with residual energy of it, $E_{res}$and its transmission range, $T_{R.}$ So neighbor nodes store this information user *i* in their storage. In future, if any wormhole attackers move 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 move 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. Thus the neighboring nodes check the message. If any node receives the any other node's transmission range is lower than the threshold value, immediately that node is noticed as an attacker node and no message is passed along that node.

Subgroup Key Generation

Table 1: Sending Energy and transmission range in subgroup generation

User I sends its public key PUi to user j

$$i \xrightarrow{PUi};\ i \rightarrow \{IDi, PUi, E^{i}_{\mathrm{Res}}, T^{i}_{R}, Ni\}$$

User j sends its public key PUj to user i

$$j \xrightarrow{PUj};\ j \rightarrow \{ID_j, PU_j, E^{j}_{\mathrm{Res}}, T^{j}_{R}, N_j\}$$

Re-keying Member Joins

Table 2: Sending Energy and Transmission Range in Key Agreement when member joins

New node S joins in the existing group G,

$$GM \xrightarrow{GK(i,j)} S$$

$$GM \rightarrow \{PU_{GM}, E^{GM}_{\mathrm{Res}}, T^{GM}_{R} PU_i, PU_j, GK(i,j), ID_{GM}, N_{GM}\}$$

User S computes public keys, $PU_{j,n}$ and $PU_{i,n}$

User S multicasts these group keys to i and j

$$S \xrightarrow{\{PUjn, PUi,n\}} i, j$$

$$S \rightarrow \{PU_S, E^{S}_{\mathrm{Res}}, T^{S}_{R} PU_{j,n}, PU_{i,n}, ID_S, N_S\}$$

Member leaves

Table 3: Sending Energy and Transmission Range in Key Agreement when member leaves

Member j leaves from existing group

Assume that old GM is 'i'

GM 'i' changes its private key PK_i and computes new public key PU_i

GM 'i' sends its public key PUi to user 'S'

$$GM \xrightarrow{PUi} S$$

$$GM \rightarrow \{PU_i, E^{i}_{\mathrm{Res}}, T^{i}_{R}, ID_i, N_i\}$$

RESULT AND DISCUSSION

Simulation study has been carried out to show the performance of the proposed Secure Hashed VBSR protocol against various attacks like blackhole, wormhole. Simulation results have been compared with different types of attacks as it has different types of secure protocols. In our simulation, test area is set as 1500mx1500m along with IEEE 802.11 MAC protocol. Various propagation parameters are considered for two ray propagation model. Transmission range is set to 250meters for 100 numbers of nodes. We have taken the packet size as 512 bytes and initial energy as 100 joules. The performance analysis is done on delay and energy consumption based on number of nodes and pause time for 20, 40 and 60 nodes.

The delay that is depicted in figure 1 and figure 2, defined as difference 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. 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 is no movement of the nodes. The delay for 20 nodes is very low however there is little movement 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 3 and figure 4. Here, the energy consumption is very high due to the count of beacons and calculation of transmitted and received beacons by every node.

When the mobility of the nodes is low for 20 nodes, the energy consumption is high because of very less computation of beacons of node movement. But for the 40 nd 60 nodes, the energy consumption is high because of node mobility.

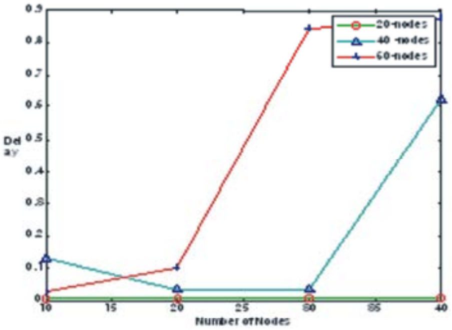

Fig 1: Variation in delay with number of nodes

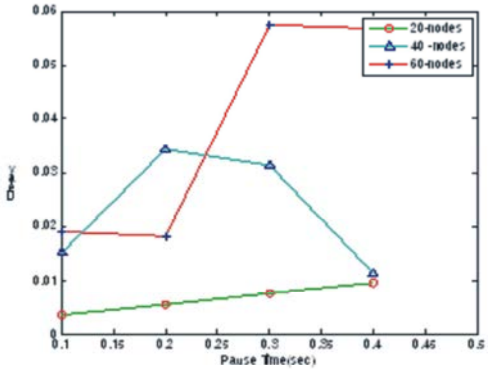

Fig 2: Variation in Delay with pause time

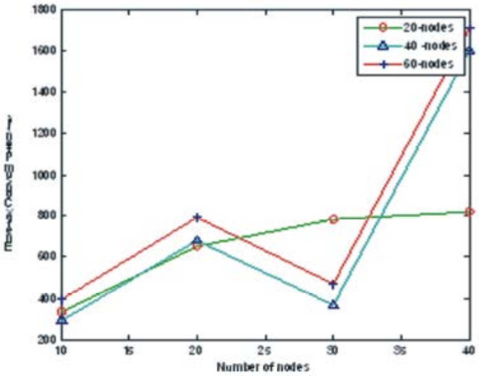

Fig 3: Energy consumption Vs Number of nodes

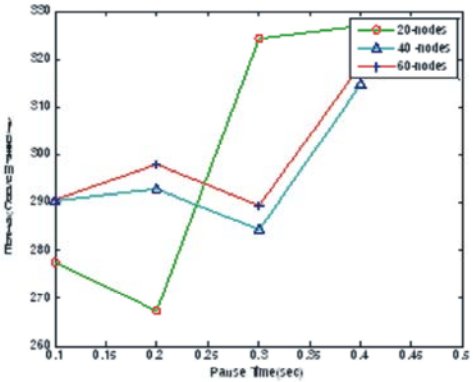

Fig 4: Energy consumption vs Pause time

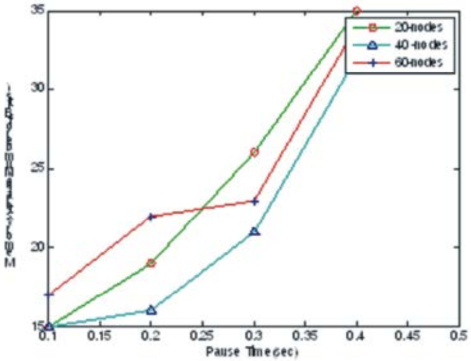

Fig 5: Variation in memory storage with pause time

The memory storage gets affected when the mobility is high and on key management, that is depicted in figure 5. 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.

CONCLUSION

Our scheme called Secure Hashed VBSR provides detailed discussion on the types of attacks and wormhole attack is detected. It is prevented by sending the energy consumption of the node and by using the transmission range of that node. By having this information, we can prevent the attack. Based on the calculated number of beacons that are received by a node and transmitted by a node, the best gateway member compared to the previous designed protocols can be selected. Also the subgroup and group keys should be rekeyed whenever the membership changes (a node is joining or leaving). The proposed scheme provides better storage, cost, energy consumption and lesser delay in terms of pause time and number of nodes.

REFERENCES

1. Ashwani Kush, P. Gupta and C. Jinshong, 2009. Hwang, Secured Routing Scheme forAdhoc Networks, International Journal of Computer Theory and Engineering, 1(3): 1793-8201.
2. Hu, Y.C., A. Perrig and D. Johnson, 2002. Ariadne: A secure on-demand routing protocol for ad hoc networks, in Proceedings of, 2002.
3. Yi, l.S. and R. Kravets, 2001. Security-aware ad hoc routing for wireless networks, in Proceedings of MobiHOC01.
4. Singh Karan, Rama Shankar Yadav and Ranvijay, 2010. A Review Paper on Ad Hoc Network Security, International Journal of Computer Science and Security, 1(1).
5. Nafeesa Begum, J., K. Kumar and Dr. V. Sumathy, 2012. Multilevel Access Control in a MANET for a Defense Messaging system using Elliptic Curve Cryptography, International Journal of Computer Science and Security, 4(2).

6. Muthumayl, K., V. Rajamani, S. Manikandan and M. Buvana, 2011. A Novel Cross layered Energy based on-demand routing protocol for Mobile ad hoc networks, IEEE International Conference on Advanced Computing, IEEE, pp: 276-281.
7. Kumar Krishnan, J. Nafeesa Begum and V. Sumathy, 2010. A Novel Approach towards Cost Effective Region-Based Group Key Agreement Protocol for Ad Hoc Networks Using Elliptic Curve Cryptography, Int. Communications, Network and System Sciences, 3: 369-379.
8. Kaabneh, K. and H. Al-Bdour, 2005. Key Exchange Protocol in Elliptic Curve Cryptography with No Public Point, American Journal of Applied Sciences, 2(8): 1232-1235.
9. Sergio Marti, T.J. Giuli, Kelvin Lai and Mary Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks, MOBICOM, MA,USA.
10. Rashid Hafeez Khokhar, MdAsri Ngadi and Satria Mandala, 0000. A Review of Current Routing Attacks in Mobile ad hoc networks, International Journal of Computer Science and Security, 2(3): 18-29.
11. Barman Roy Debdutta, Rituparna Chaki and Nabendu Chaki, 2009. A New Cluster-bases Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Networks, International Journal of Network Security & Its Applications (IJNSA), 1(1).
12. Jhaveri, Rutvij, H., Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, 2010. MANET Routing Protocols and Wormhole Attack against AODV, IJCSNS International Journal of Computer Science and Network Security, 10(4).