Journal of Computer Science 7 (7): 973-979, 2011
ISSN 1549-3636

# Impact of Sybil and Wormhole Attacks in Location Based Geographic Multicast Routing Protocol for Wireless Sensor Networks

[1]Shyamala Ramachandran and [2]Valli Shanmugan
[1]Department of Information Technology,
University College of Engineering Tindivanam,
Melpakkam-604 301, Tamil Nadu, India,
[2]Department of Computer Science and Engineering,
Faculty of Information and Communication,
College of Engineering Guindy, Anna University,
Chennai 600 025, Tamil Nadu, India

**Abstract: Problem statement:** Wireless sensor networks have been used in many applications, such as home automation, military surveillances and entity tracking systems. The sensor nodes have low computational capabilities and are highly resource constrained. Routing protocols of wireless sensor networks are prone to various routing attacks, such as black hole, rushing, wormhole, Sybil and denial of service attacks. **Approach:** The objective of this study was to examine the effects of wormhole in conjunction with Sybil attack on a location based-Geographic Multicast Routing (GMR) protocol. **Results:** The NS-2 based simulation was used in analyzing the wormhole in conjunction with Sybil attack on GMR. **Conclusion:** It is found that, the Sybil attack degrades the network performance by 24% and the wormhole attack by 20%.

**Key words:** Wireless Sensor Networks (WSN), geographic multicast routing, wormhole attack, Sybil attack, Mobile Ad-hoc Network (MANET), Geographic Multicast Routing (GMR), passive attacks

## INTRODUCTION

A Wireless Sensor Network (WSN) consists of cheap and simple processing devices, called sensor nodes. The sensor nodes have the capability of sensing parameters, such as temperature, humidity and heat. The sensor nodes communicate with each other using wireless radio devices and form a wireless sensor network. The WSN has a dynamic, continuously changing network topology which makes routing difficult. Another characteristic of the WSN is its band width and power constraints.

Silva *et al*. (2007) have implemented a traditional Multicast Ad hoc on demand Distance Vector (MAODV) on the WSN and claim that multicast routing improves the performance of the WSN. Zhang *et al*. (2006) have worked on a location aided multicast routing protocol. They use a cone-based forwarding area, through which it distributes the routing discovery process. Li *et al*. (2005) have improved the energy and reduced the delay by using spatial time division multiple access schema. Xiangli *et al*. (2008) have used a small rectangular region which covers all the forwarding nodes. The source node uses a minimal energy path for the forwarding nodes. The forwarding nodes broadcast the message to all the destination nodes in their multicast region. Therefore, early works on WSN's  focused on providing a routing service using the minimum cost in terms of bandwidth and battery power.

Zhao *et al*. (2008) have reduced the multicast transmission rate dividing the destinations into many clusters. The closest destination in each cluster receives the message and distributes it to its neighbors. Sencast (Peng *et al*., 2008) suggests a scalable, energy efficient multicast routing scheme for larger sensor groups. The works (Zhang *et al*., 2006; Li *et al*., 2005; Xiangli *et al*., 2008; Zhao *et al*., 2008; Peng *et al*., 2008) rely on the cooperation between the nodes. These approaches assumed that all the nodes are trustworthy and well-behaved. However, sensor applications deploy the sensor nodes randomly, which causes the nodes to be unattended. It raises the problem of secure administration and utilization.

**Corresponding Author:** R. Shyamala, Department of Information Technology, University College of Engineering Tindivanam-604 301, Tamil Nadu, India

The attacks on the WSN are classified into active attacks and passive attacks. The monitoring and listening of the communication channel by unauthorized attackers are known as passive attacks. The attack against privacy is passive in nature. Some of the more common attacks against sensor privacy are monitoring and eavesdropping, traffic analysis and camouflage adversaries. If the unauthorized attackers monitor, listen to and modify the data stream in the communication channel, then the attack is an active one. Routing attacks such as spoofing, replay, selective forwarding, sinkhole, Sybil, wormhole and HELLO flood are active attacks. Denial of service attacks, such as neglect and greed, misdirection, black hole are also active in nature.

Kannhavong *et al*. (2007) have handled flooding, black hole, link withholding, link spoofing, replay, wormhole and colluding misrelay attacks on Mobile Ad-hoc Network (MANET) routing protocols. Coskun and Levi (2006) deal with a secured multicast routing protocol that controls the spam attacks. The spam attacker aims at exhausting the battery power of the sensor node and causes extra delay in the network. Nguyen and Nguyen (2007) in their study, classify rushing, black hole, neighbor and jelly fish as severe routing attacks on the WSN. Viswanatham and Chari (2008) analyzed various threats in mobile ad hoc networks by a mobile agent in the AODV protocol. Bhalaji *et al*. (2008) have given a relationship estimator technique to enhance Dynamic Source Routing (DSR). By this trust relationship model, malicious nodes have been identified and isolated from route detection in mobile ad hoc networks. Murugam and Shanmugam (2010) have suggested a cumulative isolation technique to detect MAC and routing attacks in mobile ad hoc networks. Sharif and Ahmed (2010) have found that the existing routing protocols were more inefficient against a wormhole attack on the WSN. In the previous work (Shyamala and Valli, 2009) a TESLA based secure route discovery is suggested for MAODV. Hanapi *et al*. (2009) have suggested a secured routing algorithm which, uses a lazy binding technique and dynamic time on collection window and applies a geographical routing techniques.

This study simulates the wormhole attack in conjunction with the Sybil attack in Geographic Multicast Routing (GMR). The simulation was carried out using NS-2 and the network performance is studied with and without worm hole and Sybil attack in the WSN.

## MATERIALS AND METHODS

**Geographic multicast routing protocol:** Depending on the network structure, routing in WSNs can be divided into flat-based routing, hierarchical-based routing and location-based routing. Sensor Protocols for Information via Negotiation (SPIN), directed diffusion and rumor routing are examples of flat routing. Low Energy Adaptive Cluster Hierarchy (LEACH), LEACH Centralized (LEACH-C), Power Efficient Gathering In Sensor Information System (PEGASIS) are hierarchical routing protocols.

Sanchez *et al*. (2007) proposed an energy efficient routing protocol for the WSN, called the Geographic Multicast Routing Protocol (GMR). The GMR is a location based protocol. The GMR protocol can calculate the position of the sensor nodes from the Global Positioning System (GPS) (Xu *et al*., 2008) or it can use the virtual co-ordinates. Each sensor node communicates its position to its neighbors using periodic beacons. The GMR forms a multicast tree to send a data packet from a source to multiple destinations, using a single broadcast transmission.

In the GMR, each forwarding node selects a subset of its neighbors in the direction of the destination as relay nodes, based on the cost over progress ratio. The cost is equal to the number of selected neighbors. Progress is the reduction of the remaining distance to the destination. The cost over progress metric is explained with respect to Fig. 1. The remote source node S multicasts the message M to a set of destinations {D1, D2, D3, D4, D5}. The forwarding node C receives the message M from the source S and uses its neighbors $A_1$, $A_2$ as the relay nodes. In the GMR, the multicasting task could be given to one neighbor or it could be split and given to several neighbors. Each neighbor could address a set of destinations.

From node C the total distance for multicasting is $T_1$ as given in Eq. 1. Then the node C applies the greedy partitioning algorithm and selects $A_1$ as the relay node responsible for $D_1$, $D_2$ and $D_{3.}$ The node $A_2$ is chosen as the relay node for $D_4$ and $D_{5.}$ For the next level of the multicast tree, a new total distance $T_2$ is calculated as given in Eq. 2. The progress is the difference between $T_1$ and $T_2$ as given in Eq. 3. The cost over progress ratio $P_i$ for the new forwarding set $\{A_{1,}\ A_2\}$ is given by Eq. 3.

The node C informs its neighbors that they are selected as the relay nodes through the header. The header format is given in Fig. 2. The GMR adds this header to the data message:

$$T_1= |CD_1|+|CD_2|+|CD_3|+|CD_4|+|CD_5| \quad (1)$$

$$T_2=|A_1D_1|+|A_1D_2|+|A_1D_3|+|A_2D_4|+|A_2D_5| \quad (2)$$

$$P_i =2 / T_1 -T_2 \quad (3)$$

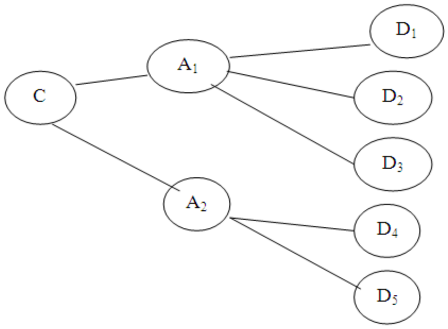
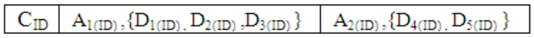
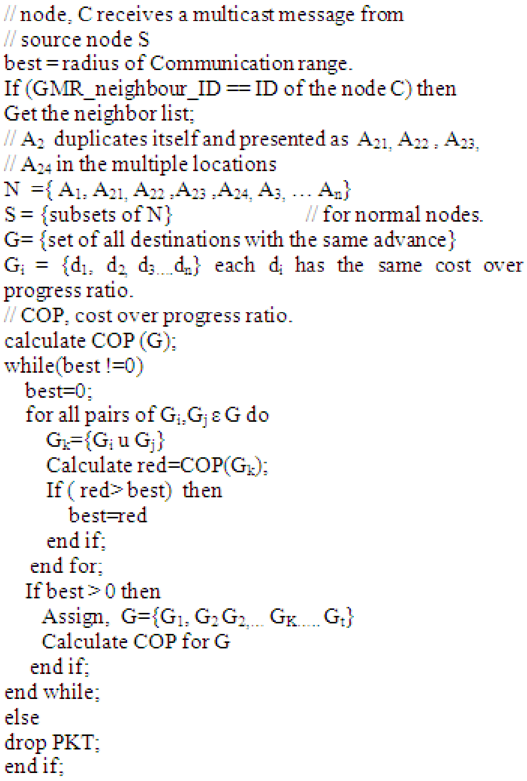


Fig. 1: GMR-Neighbor Selection



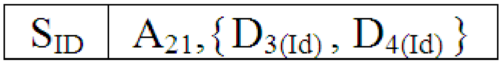
| | | |
|---|---|---|
| $C_{ID}$ | $A_{1(ID)}$ ,{$D_{1(ID)}$ , $D_{2(ID)}$ ,$D_{3(ID)}$ } | $A_{2(ID)}$ ,{$D_{4(ID)}$ , $D_{5(ID)}$ } |

Fig. 2: Header format



```
// node, C receives a multicast message from
// source node S
best = radius of Communication range.
If (GMR_neighbour_ID == ID of the node C) then
Get the neighbor list;
// $A_2$ duplicates itself and presented as $A_{21}$, $A_{22}$ , $A_{23}$,
// $A_{24}$ in the multiple locations
N ={ $A_1$, $A_{21}$, $A_{22}$ ,$A_{23}$ ,$A_{24}$, $A_3$, … $A_n$}
S = {subsets of N}                        // for normal nodes.
G= {set of all destinations with the same advance}
$G_i$ = {$d_1$, $d_2$, $d_3$...$d_n$} each $d_i$ has the same cost over
progress ratio.
// COP, cost over progress ratio.
calculate COP (G);
while(best !=0)
   best=0;
   for all pairs of $G_i$,$G_j$ ε G do
      $G_k$={$G_i$ u $G_j$}
      Calculate red=COP($G_k$);
      If ( red> best) then
         best=red
      end if;
   end for;
   If best > 0 then
     Assign, G={$G_1$, $G_2$ $G_2$,... $G_K$..... $G_t$}
     Calculate COP for G
   end if;
end while;
else
drop PKT;
end if;
```

Fig. 3: Pseudo code for the Sybil attack



| | |
|---|---|
| $S_{ID}$ | $A_{21}$,{ $D_{3(Id)}$ , $D_{4(Id)}$ } |

Fig. 4: Sybil attack header format

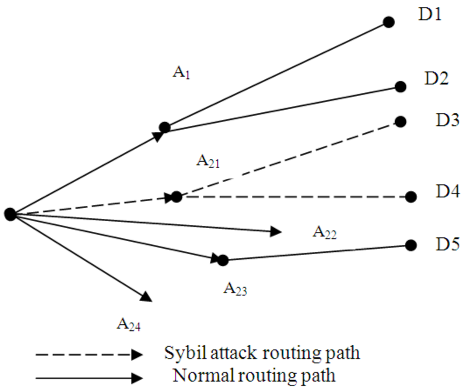


Fig. 5: Sybil attack

Thus the sender broadcasts a single message and it reaches the destination by selective forwarding and hence the energy and bandwidth consumption is minimized.

**Sybil attack on the GMR:** When the malicious node illegitimately takes on multiple identities, it is a Sybil attack (Xiao *et al*., 2009). A single node duplicates its ID and presents it at multiple locations. The node, which presents multiple identities to other nodes in the network, could be the malicious node. The traffic migrates into that malicious node and this can significantly reduce the effectiveness of fault tolerant schemes, such as distributed storage, dispersity and multipath. A Sybil attack has two stages. In the first stage, the node exploits the routing protocol to advertise itself as having a valid route to the destination, even though the route is spurious. In the second stage, the node consumes the intercepted packets for a replay, wormhole or sinkhole attack.

This work implements the Sybil attack in the GMR protocol. During the normal operation, the node advertises its ID and location information to its one hop neighbor by a beacon message. Since there is no authentication in the GMR, the duplicate nodes also participate in multicasting. The cost over progress ratio is calculated. The malicious node M exhibits high energy and minimal distance, as compared to the normal node. It starts the attack from the root of the multicast tree. The Greedy partitioning algorithm of the GMR (Sanchez *et al*., 2007) selects node M as a relay node, since it has the best cost over progress ratio. Figure 3 is the pseudo code for implementing a Sybil attack in the GMR protocol. Figure 4 is the data header format and Fig. 5 is an example of a Sybil attack.

In the following algorithm the neighbor node with the best cost over progress ratio is taken as the forwarding node for the routing. For instance, node C receives a multicast message from its neighbour node A. Node C reads the header and gets the forwarding node's ID. If it finds its ID, then it starts calculating the cost over progress ratio. Node C gets the neighbor's ID list N. Initially, the best distance between node C and all its neighbors is set high (i.e., equal to the radius of the communication range of node C). The set of all subsets of N forms a set S. In the subset, each node $n_i$ which has the same distance from C is retained in the same subset $S_i$. D is a set of all destinations of the multicast message. Set G is equal to the set of all destinations with the same distance from node C. For each element of $S_i$ the cost over progress ratio for all the subsets of G is calculated. $G_i$ and $G_j$ are the subsets of G. Set $G_i$ is merged with $G_j$ if for any subset of $S_i$ the subsets $G_i$ and $G_j$ provide a higher improvement in the overall cost over progress ratio. This procedure is repeated for all the subsets of S and G. The resultant S forms the relay node for the set of destinations D.

The header consists of the source ID, the relay node ID and sets all destinations' IDs that can be reached via the relay node. In the GMR, the source node initiates a data message for the set of destinations. Each node requires $O\ (D,n)^3$ (where, D is the number of destinations and n is the number of neighbors of the node currently multicasting the message) forwarding node selection time, in the worst case. In a wormhole attack, the malicious node creates a Sybil attack and attracts the traffic towards it. In the next step, it rushes the data message to its neighbor, who is far away. This reduces the ability to forward a legitimate data message and exhausts the battery power for unwanted computation. It introduces a longer network delay.

**Wormhole attack on the GMR:** A wormhole attack (Hu *et al*., 2006) is one of the most sophisticated and severe attacks on the WSN. In this attack, a pair of colluding attackers records packets at one location and replays them at another location using a private high speed network. An attack launcher situated close to a base station may be able to completely disrupt the routing by creating a well-placed wormhole. An adversary could convince the nodes that would normally be at multiple hops from a base station, that they are only one or two hops away via the wormhole.

This study studies the wormhole attack in terms of its effect on the operation of the GMR.

## RESULTS AND DISCUSSION

**Simulation environment:** To evaluate the effectiveness of the proposed attacks, the GMR is simulated using NS-2 (Downard, 2004). The goal of the evaluation is to test the effectiveness of the Sybil and wormhole attack variations under normal conditions. The size of the data payload is 512 bytes. The simulation is based on 200 nodes. Nodes 11-200 are simple nodes and nodes 1-10 are the malicious nodes. Table 1 shows the simulation parameters. The number of malicious nodes was varied from 2-10 and the results are given in Table 2-3.

The network performance is evaluated using the packet delivery ratio, network throughput, packet drop ratio and energy loss metrics in the presence of Sybil and wormhole attacks.

**Performance analysis: Packet delivery ratio:** Packet Delivery Ratio (PDR) is defined as the ratio of the total number of data packets received by the destination node to the number of data packets sent by the source node.

Figure 6 represents the packet delivery ratio of the GMR protocol. The packet delivery ratio drastically decreases, when there is a malicious node in the network. For example, the packet delivery ratio is 100% when there is no effect. From Fig. 6, due to the Sybil attack, the packet delivery ratio decreases to 77%, because some of the packets are consumed by the duplicate node. In case of a worm hole attack the PDR decreases to 85% because of fast message forwarding.

**Network throughput:** The network throughput represents the ratio between the number of data packets generated from the source node, to the number of data packets received at the destination in percentage in Fig. 7. The throughput of the network is 100% when there is no attack. The GMR seems to be resistant to a wormhole attack since the throughput is reduced by 15%, whereas the Sybil attack reduces the throughput by 20%. At 100 ms the Sybil attack reduces the throughput to 60% and it remains at the same value for the next 150 ms. Later than that, the throughput is regularly decreased. Once, the Sybil attack is launched it creates multiple identities. These malicious nodes take part in routing and consume the data packets. When the time proceeds these nodes are slowly removed from the routing path and hence the throughput becomes constant.

To initiate a wormhole it takes 150 ms. Once it has been launched the value of the throughput is reduced to 50% from the normal value as given in Fig. 7.

**Packet drop:** Packet drop is the average number of packets dropped by the network. Figure 8, shows the results of packet loss for the wormhole and the Sybil attack.

Table 1: Simulation Parameters

| Examined Protocol | GMR |
|---|---|
| Simulator | NS-2 |
| Smulation time | 250 sec |
| Simulation area | 1000×1000m |
| Number of sensor nodes | 200 |
| Number of base stations | 1 |
| Number of malicious nodes | 5 |
| Transmission range | 250m |
| Movement model | Static |
| Initial energy | 5J |
| RxPower | 1.75mW |
| TxPower | 1.75mW |
| SensePower | 1.75mW |
| IdlePower | 1.75*u*W |

Table 2: Average performance of the GMR for varying number of malicious nodes in a Sybil attack

| No. of malicious node | packet delivery ratio $\times 10^{-3}$ | average delay $\times 10^{-3}$ | energy consumed (joules) | energy loss (joules) |
|---|---|---|---|---|
| 10 | 5.76 | 5.0 | 1.67 | 3.33 |
| 8 | 4.78 | 5.0 | 1.55 | 3.45 |
| 6 | 4.08 | 4.7 | 1.52 | 3.48 |
| 4 | 3.54 | 4.3 | 1.40 | 3.60 |
| 2 | 3.17 | 4.1 | 1.28 | 3.72 |

Table 3: Average performance of the GMR for varying number of malicious nodes in a wormhole attack

| No. of malicious node | Packet delivery ratio $\times 10^{-3}$ | Average delay $\times 10^{-3}$ | Energy consumed (joules) | Energy loss (joules) |
|---|---|---|---|---|
| 10 | 4.05 | 3.2 | 2.57 | 2.43 |
| 8 | 3.55 | 2.5 | 2.00 | 3.00 |
| 6 | 3.05 | 2.1 | 1.47 | 3.53 |
| 4 | 3.48 | 1.7 | 1.32 | 3.68 |
| 2 | 2.47 | 1.2 | 1.12 | 3.88 |

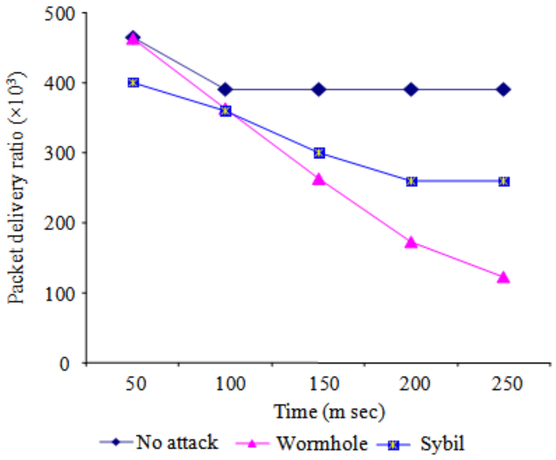


Fig. 6: Packet delivery ratio

The Sybil attack drops more number of packets at its initialization. Multiple images of the same nodes take part in routing, which observes the packets and drop it.

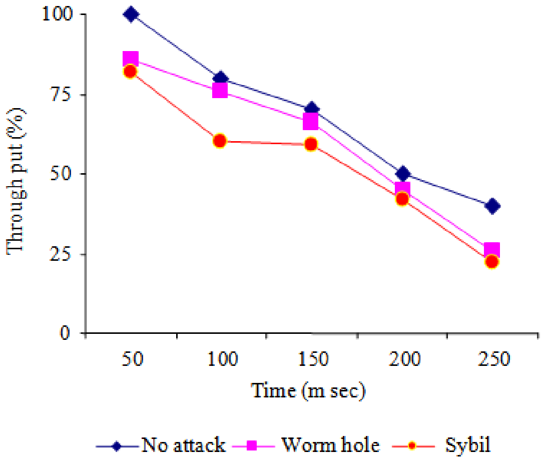


Fig. 7: Network throughput

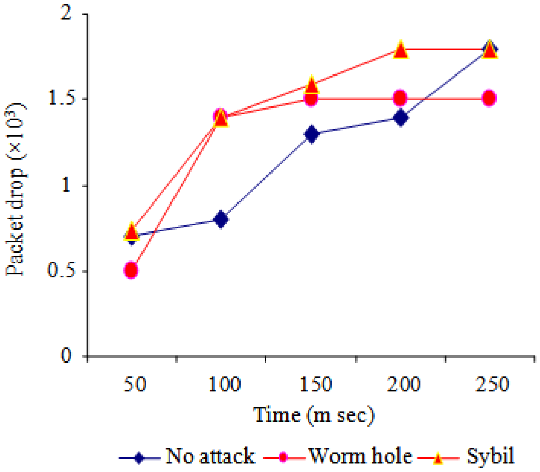


Fig. 8: Packet drop ratio

Once the Sybil attack is on track, the packet loss is uniform for the subsequent 150 ms. The wormhole attack was commenced at 150 ms, the packet loss at that moment is about twice the value of no attack due to the malicious nodes, which tunnel the data packets from one part of the network to other. As a result, the destination nodes do not receive the sent packet.

**End to end delay:** Figure 9, shows the end to end delay. The average end to end delay for multicast is uniform when there is no attack. The wormhole attack in its extensiveness at 150 ms steals the message from the source node. Therefore, the average end to end delay increased to 40%. In the Sybil attack, the delay is 10% for every 50 ms when compared to the multicast with no attack. From, this result it is observed that the worm hole requires an extremely tight time synchronization between the sensor node and the base station during routing. A strong routing message authentication and encryption reduces the worm and Sybil attacks.

**Energy consumption:** Figure 10 shows the energy consumption of a network for the worm hole, Sybil and for the normal operation of the GMR multicast protocol. The energy consumption of the network varies from 5-1 joule in the case of no attack.

For the wormhole attack the network drops its energy to 0.5 joules. From these values, it is observed that the battery power of the sensor nodes was highly drained by the malicious nodes. In the Sybil attack the duplicate nodes start troubling the routing, by which it drains the overall network energy at 100-150 ms. From 200 ms of simulation, the energy consumption of the network is 10% more than that under normal operation.

Table 2-3 show the values obtained, when the numbers of the malicious nodes are 2, 4, 6, 8 and 10 respectively. The average performances of the packet delivery ratio, network delay, energy consumption, energy loss were noted. From the results it is observed that the Sybil attack degrades the performance of the GMR on a large scale, when compared to a worm hole attack.

Table 2-3, show the average performance of the GMR for varying number of malicious nodes (n). For n = 2, the packet delivery ratio is high in a Sybil attack when compared to a wormhole, because, the wormhole consumes more number of packets. But, the proportional drop in the packet delivery ratio for the worm hole is less, compared to the Sybil because, the multiple identities of the Sybil node disturb the routing procedure and it consumes more number of packets. The average delay for the wormhole is low when compared to the Sybil, since a malicious node transfers the packet to other parts of network through a powerful link communication channel. In the Sybil attack, a malicious node creates multiple identities and each duplicate node consumes a packet, which causes an overall increase in average delay. The energy consumption for the Sybil and wormhole is almost the same. From this data, it is implicit that the wormhole attack causes more damage to the routing procedure of the GMR than the Sybil attack.

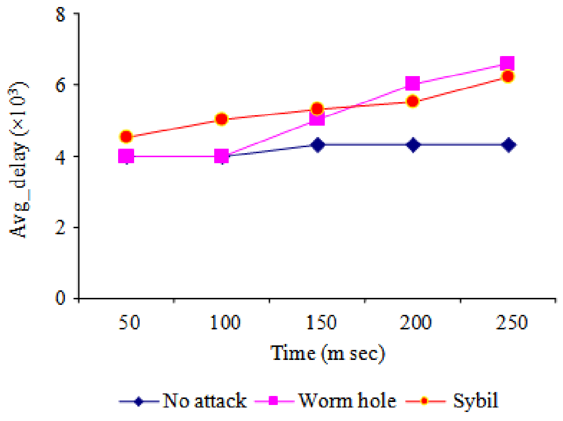


Fig. 9: End to end delay

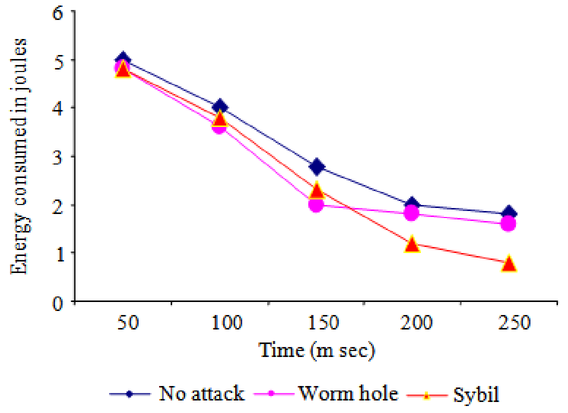


Fig. 10: Energy loss

## CONCLUSION

With developments in WSN environments, the services based on the WSN have been increased. In this study the effect of the wormhole in conjunction with the Sybil attack on the GMR have been studied. The packet delivery ratio, throughput, end-to-end delay and energy loss have been evaluated. There is a reduction in the packet delivery ratio, throughput and end to end delay as observed from the graphs. Having considered the wormhole and Sybil attacks in the GMR, it is evident that it is extremely necessary to control these routing attacks. So, the task of providing secure routing for Wireless sensor networks presents a rich field for researchers.

## REFERENCES

Bhalaji, N., S.Banerjee and A. Shanmugam, 2008. A novel routing technique against packet dropping attack in adhoc networks. J. Comput. Sci., 4:538-544. DOI: 10.3844/jcssp.2008.538.544

Coskun, V. and A. Levi, 2006. Quarantine region scheme to mitigate spam attacks in wireless sensor networks. IEEE Trans. Mobile Comput., 5:1074-1086. DOI: 10.1109/TMC.2006.121

Downard, I., 2004. Simulating Sensor Networks in NS-2 NRL/FR/5522--04-10073, Naval Research Laboratory, Washington, D.C. http://cs.itd.nrl.navy.mil/work/sensorsim/index.php

Hanapi, Z.M., M. Ismail and K. Jumari, 2009. Priority and Random Selection for Dynamic Window Secured Implicit Geographic Routing in Wireless Sensor Network. Am. J. Eng. Applied Sci., 2: 494-500. DOI: 10.3844/ajeassp.2009.494.500

Hu, Y.-C., A. Perrig and D.B. Johnson, 2006. Wormhole attacks in wireless networks. IEEE J. Selected Areas Commun., 24: 370-380. DOI: 10.1109/JSAC.2005.861394

Kannhavong, B., H. Nakayama, Y. Nemoto and N. Kato, 2007. A survey of routing attacks in mobile ad hoc networks. IEEE Wireless Commun., 14: 85-91. DOI: 10.1109/MWC.2007.4396947

Li, Z., W. Zhang, H.C. Liu, B. Zhao and Y. Qu, 2005. Multicast routing with minimum energy cost and minimum delay in wireless sensor networks. In Lecturer Notes Embedded Ubiquitous Comput., 3823: 1157-1168. DOI: 10.1007/11596042_118

Murugam, R and A. Shanmugam, 2010. A combined solution for routing and medium access control layer attacks in Mobile Ad Hoc networkx. J. Comput. Sci., 6: 1416-1423. http://thescipub.com/pdf/10.3844/jcssp.2010.1416.1423

Nguyen, H.L. and U.T. Nguyen, 2008. A study of different types of attacks on multicast in mobile ad hoc networks. J. Ad Hoc Networks., 6: 32-46. DOI: 10.1109/ICNICONSMCL.2006.202

Peng, S., S. Li, L. Chen, N. Xiao and Y. Peng, 2008. SenCast: Scalable multicast in wireless sensor networks. IEEE Proceeding of the Parallel and Distributed Processing, Apr. 14-18, Miami, FL., pp: 1-9. DOI: 10.1109/IPDPS.2008.4536255

Silva, S.J., T. Camilo, A. Rodrigues, M. Silva. F Gaudencio, F. Boavida, 2007. Multicast in wireless sensor networks the next step. Proceeding of the Wireless Pervasive Computing, Feb. 5-7, San Juan, pp: 47-55. DOI: 10.1109/ISWPC.2007.342598

Sanchez, J.A. Ruiz and P.M. Stojmnenovic, 2007. GMR: Geographic multicast routing for wireless sensor networks. J. Comput. Commun., 30: 2519-2531. DOI: 10.1016/j.comcom.2007.05.032

Sharif, L. and M. Ahmed, 2010. The wormhole routing attack in Wireless Sensor Networks (WSN). J. Inform. Process. Syst., 6: 177-184. DOI: 10.3745/JIPS.2010.6.2.163

Shyamala. R. and S. Valli, 2009. Secure route discovery in MAODV for wireless sensor networks. UbiCC J., 4: 775-783. www.ubicc.org/files/pdf/4_289.pdf

Viswanatham, V.M and A.A Chari, 2008. An approach for detecting attacks in mobile ad hoc networks. J. Comput. Sci., 4: 245-251. DOI: 10.3844/jcssp.2008.245.251

Xiangli, W., L. Layuan and W. Wenbo, 2008. An energy-efficiency multicast routing algorithm in wireless sensor networks. Proceedings of the on Computing, Communication, Control and Management, Aug. 3-4, Guangzhou, pp: 572-576. DOI: 10.1109/CCCM.2008.239

Xiao, L., L.J. Greenstein, N.B. Mandayam, 2009. Wade trappe, channel-based detection of Sybil attacks in wireless networks. IEEE Trans. Inform. Forensics Security, 4: 492-503. DOI: 10.1109/TIFS.2009.2026454

Xu, L., Z. Deng, W. Ren, H.W. Sch, 2008. A location algorithm integrating GPS and WSN in Pervasive Computing. In Pervasive Comput. Appli., 1 : 461-466. DOI: 10.1109/ICPCA.2008.4783632

Zhang, W., X. Jia and C. Huang, 2006. Distributed energy-efficient geographic multicast for wireless sensor networks source. Int. J. Wireless Mobile Comput., 1: 141-147. DOI: 10.1504/IJWMC.2006.012473

Zhao, G., X. Liu and A. Kumar, 2008. Geographic multicast with k-means clustering for wireless sensor networks. Proceedings of the IEEE Conference on Vehicular Technology, May 11-14, Singapore, pp: 233-237. DOI: 10.1109/VETECS.2008.60