PERFORMANCE COMPARISON OF ROUTING ATTACKS IN MANET AND WSN

Shyamala Ramachandran[1], Valli Shanmugam[2]

[1] Assistant Professor, Department of Information Technology,
University College of Engineering Tindivanam, Melpakkam 604 001.
vasuchaaru@gmail.com
[2]Associate Professor, Department of Computer Science and Engineering,
Anna University, Chennai-25.
valli@annauniv.edu

ABSTRACT

Routing is a basic step for data exchange. In wireless ad-hoc networks each node acts as a router and executes a routing protocol. Wireless ad-hoc networks are highly resource constrained in terms of network topology, memory and computation power. The reliable data transfer is a difficult task in wireless ad-hoc networks because of resource constraints. A mobile ad-hoc network (MANET) is a kind of wireless ad-hoc network, and is a self-configuring network of mobile routers connected by wireless links. A wireless sensor network (WSN) is a highly constrained wireless ad-hoc network. In these network, multicast is the efficient routing service for data broadcasting. Denial of service (DOS) attack, sinkhole, wormhole, sybil, black hole and rushing attacks are some routing attacks. So, it is necessary to study the impact of routing attacks on existing multicast routing protocols to suggest a suitable secure multicast routing protocol. The objective of this paper is to study the effects of black hole and rushing attack on MANET and WSN. The NS-2 based simulation is used in analyzing the black hole and rushing attacks. From performance metrics such as packet delivery ratio (PDR), packet drop ratio (PDrR), network throughput (NTh) and energy consumption it is observed that the routing attacks have severe impact on MANET than WSN.

KEYWORDS

Wireless sensor networks, MANET, multicast routing, black hole attack, joules & throughput.

1. INTRODUCTION

A mobile ad-hoc network (MANET) has self – organizing mobile nodes that communicate with each other via wireless links with no infrastructure. Nodes in a MANET operate both as hosts as well as routers to forward packets to each other. MANETS are suitable for applications, in which no infrastructure exists such as military, emergency rescue and mining operations. A wireless sensor network (WSN) consists of sensor nodes which are simple processing devices. The sensor nodes have the capability of sensing parameters like temperature, humidity and heat. The sensor nodes [1] communicate with each other using wireless radio devices and form a WSN. The WSN is dynamic and has a continuous changing network topology which makes routing difficult. Bandwidth and power limitations are the important resource constraints.

The authors [2], classify the attacks on WSN as active 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 and modify the data stream in the communication channel, then the attack is active attack. Routing attacks such as spoofing, replay, selective

DOI : 10.5121/ijasuc.2012.3405

forwarding, sinkhole, sybil, wormhole, HELLO flood are active attacks. Denial of service attacks such as neglect and greed, misdirection, black hole are also active in nature.

Hoang and Uyen [3] in their study, classify the rushing, black hole, neighbor and jelly fish as the severe routing attacks in MANET. The impact of routing attacks was studied by varying the number of senders and receivers. From the results it is shown that the rushing attack causes more damage to the routing irrespective of number of senders and receivers. In case of black hole attack, if the attacker is closer to the destination heavy damage is caused to the network. According to Hoang et al a large mesh MANET has negligible damage from any type of routing attacks. Kannhavong et al [4] have handled flooding, black hole, link withholding, link spoofing, replay, wormhole and colluding misrelay attacks on Mobile ad-hoc network(MANET) routing protocols. Avinash et al [5] used a non cooperative game theory to identify black hole nodes and proposed a new Ad-hoc On-demand Distance Vector (AODV) routing protocol for Mobile Ad-hoc network (MANET). Jorge et al [6] used watchdog and Bayesian filters to detect black hole attack by means of which malicious nodes are identified in MANET. Anoosha et al [7] identified black holes using honey pot agents. This roaming software agent performs a network tour and identifies the malicious node through route request advertisements and maintains intrusion logs. Kai et al [8] proposed a energy efficient, denial of service (DoS) and flooding attack resistant routing protocol using ant colony optimization. In this algorithm every node has a trust value. Faithful forwarding nodes are selected based on the remaining energy and trust value. Guoxing et al [9] proposed a trust aware secure multi-hop routing protocol for WSN. The trust values are calculated by exploiting the replay of routing information by which all the malicious nodes are dropped from routing decisions. In the previous work [13] a TESLA based secure route discovery is suggested for MAODV. The sybil and wormhole attack [16] is investigated in GMR for WSN. It is found that wormhole attack does more damage than sybil attack on the routing procedure.

This paper simulates the black hole and rushing attack in Geographic Multicast Routing (GMR). The simulation was carried out using NS-2 and the network performance is studied with and without black hole and rushing attack in the WSN and a comparison is made with MANET based on the study of Hoang et al[3].

The rest of this paper is organized as follows. Section 2, describes the Geographic Multicast Routing protocol (GMR). Section 3 describes the rushing attack. Section 4 describes the black hole attack. Section 5 describes the simulation environment and analyses the performance of the network in the presence and absence of black hole and rushing attack and section 6 concludes the work.

2. 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 algorithm. Sensor protocols for information via negotiation (SPIN), directed diffusion and rumor routing are some of the flat-based routing algorithms. Low energy adaptive cluster hierarchy (LEACH), leach centralized (LEACH-C), power efficient gathering in sensor information system (PEGASIS) are the hierarchical routing protocols.

Sancez et al [10] proposed an energy efficient routing protocol for WSN called Geographic Multicast Routing Protocol (GMR) which is one of the location based protocol. The GMR protocol calculates the position of the sensor nodes from Global Positioning System (GPS) [11] or it can use the virtual co-ordinates. Each sensor node communicates its position to its neighbors using periodic beacons. GMR forms a multicast tree to send a data packet from a source to multiple destinations using a single broad cast transmission.

In GMR [10], each forwarding node selects a subset of its neighbors in the direction of the destination as relay nodes based on cost over progress ratio. The cost is equal to the number of selected neighbors. Progress is the reduction of the remaining distances to the destinations. The cost over progress metric is explained with respect to Figure 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 neighbours A_1 and A_2 as the relay nodes. In GMR, the multicasting task could be given to one neighbor or it could be handled by several neighbors. Each neighbor could address a set of destinations.

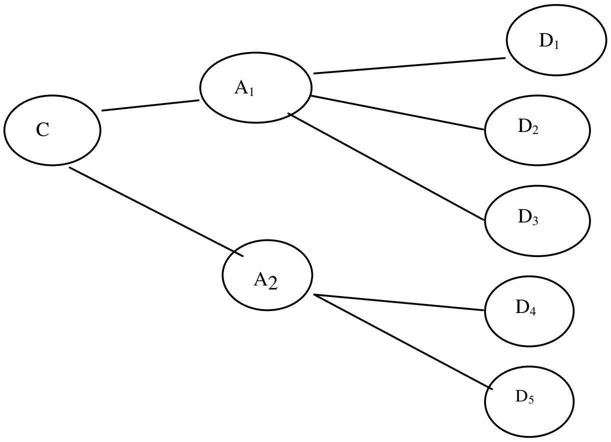

Figure 1 GMR – Neighbor Selection

From node C the total distance for multicasting is T_1 as given in equation (1). Then the node C applies 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 equation (2). The progress is the difference between T_1 and T_2 as given in equation (3). The cost over progress ratio (P_i) for the new forwarding set $\{A_1, A_2\}$ is $2/ T_1 - T_2$. The node C informs its neighbors that they are selected as the relay nodes through the header, given in Figure 2. The GMR adds this header to the data message.

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

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

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

C_{ID}	$A_{1(Id)}$,{$D_{1(Id)}$, $D_{2(id)}$,$D_{3(id)}$ }	$A_{2(Id)}$,{$D_{4(Id)}$, $D_{5(id)}$ }

Figure 2 Header Format

In Figure 2, the first field is the node, namely node C, which applies the greedy partitioning algorithm. The next field is the first relay node A_1 and the set of destinations it has to handle $\{D_1, D_2, D_3\}$. The third field is the second relay node, A_2 and the set of destinations $\{D_4, D_5\}$. Thus the sender broadcasts a single message and it reaches the destination by selective forwarding. Hence, energy and bandwidth consumption are minimized.

3. RUSHING ATTACK IN GMR

Rushing attack [3] is a kind of denial of service attack. When the source node floods the network with route discovery packets to find routes to the destinations, each intermediate node processes only the first non-duplicate packet and discards the other duplicate packets that arrive at a later time. A rushing attacker exploits this duplicate suppression mechanism by quickly forwarding route discovery packets in order to gain access to the forwarding group.

This paper studies the rushing attack in terms of its effect on the operation of GMR. In this implementation the GMR is implemented with a source node(C) that initiates a data message to 20 destinations. The malicious nodes are uniformly distributed throughout the network. The cost over progress ratio is calculated. In this simulation, rushing attack is introduced by setting data packets processing delay time to 10 ms for all the good nodes. For rushing nodes (M) the processing delay time is set to zero. Therefore, node M_i is chosen as the forwarding node by the Greedy partitioning algorithm of GMR [10]. The malicious node M_i is chosen as the relay node since it has the best cost over progress ratio. From this experimentation, it has been found that the introduced malicious nodes will be selected as the forwarding nodes. Figure 3 is the pseudo code of rushing attack in GMR.

```
RUSHING(M: Set of malicious node)
begin
for all nodes do
set bestCOP = 0;
end for;
$M=\{M_1,M_2,M_3,\ldots M_n\}$, Where, $M_i$ = Malicious Node i
for i=1 to n do
    Set Processing Delay as 0 for $M_i$          // Malicious nodes
end for
for i =1 to n do
    Set Processing Delay as 10 ms for $N_i$          // Normal nodes
end for;
// node C receives a multicast message from source node S
If (GMR_neighbour_ID = = ID of node C) then
    Get the neighbor list (A)
    for i = 0 to k do // k  neighbors ($A_i$) of C
        for j = 0 to m do // m  destination ($D_j$)
            CurrentDistance (i,j)  - = distance ($A_i$, C) + distance ($D_j$, $A_i$);
//check
        end for                    //for j;
        Progress($P_i$) = Min(CurrentDistance(i,j) );
        Calculate Cost($A_i$) = Packet_arrival_time((C,$A_i$))
        newCOP=Cost($A_i$) / Progess($P_i$)
        if COP($A_i$) > newCOP($A_i$)
            bestCOP($A_i$)=newCOP($A_i$)
        end if
    end for                              //for i;
else
    drop PKT;
end if;
```

Figure 3 Pseudo code for rushing attack.

4. BLACK HOLE ATTACK IN GMR

When all the messages are redirected to a specific node, it is defined as black hole attack [12]. The node could be the malicious node. The traffic migrates into that malicious node. The node would not exist after a black hole attack. A black hole attack has two stages. In the first stage, the black hole 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 and suddenly disappears.

This paper implements the black hole attack in GMR protocol using the pseudo code given in Figure 4. A set of malicious nodes(M) with the processing delay of 0 ms is launched and normal nodes are set with a processing delay of 10 ms. The black hole node advertises its ID and location information to its one hop neighbor by a beacon message. Then, GMR partition algorithm is executed. Since, black hole nodes has less processing delay and hence best cost over progress ratio (COP) they are selected as the relay nodes. In our implementation only 6 nodes were selected as the forwarding nodes in the first iteration. So, the loop is repeated until all the 10 malicious nodes are selected as the forwarding nodes in the multicast tree. At 100 ms of simulation time, the malicious node starts dropping the packets. When 200ms is reached the energy is set to zero. So, the black hole node disappears from the multicast tree. Figure 5 is a example of black hole attack and Figure 6 is the data header format.

```
BLACKHOLE( M: set of Malicious Node )
repeat
        RUSHING(M);
Until all malicious nodes are selected as forwarding nodes.
if (Simulation time = = 100ms) then
        M drops PKT.
else
        if  (Simulation time = = 200ms) then
                for i = 1 to n  do
                        Set energy of $M_i$ as 0;
                end for;
        end if;
end if;
```

Figure 4 Pseudo code for Black hole attack

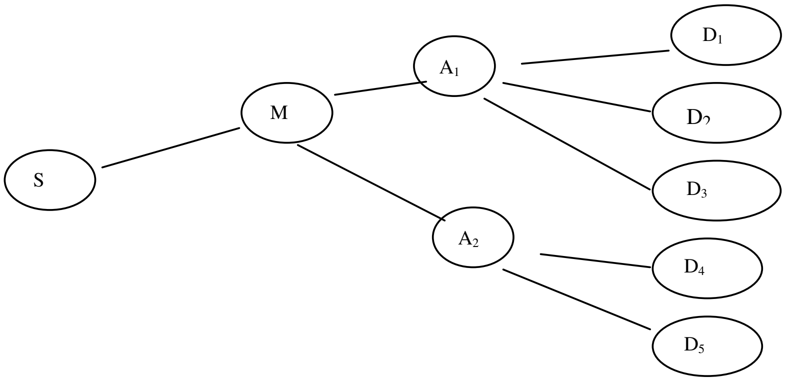

Figure 5 Black hole attack

S_{ID}	M_{ID},{$D_{1(Id)}$, $D_{2(Id)}$, $D_{3(Id)}$, $D_{4(Id)}$, $D_{5(Id)}$ }

Figure 6 Black hole Header Format

5. SIMULATION ENVIRONMENT

To evaluate the effectiveness of the proposed attacks, the GMR is simulated using NS-2[13, 14]. The goal of the evaluation is to test the effectiveness of the black hole and rushing attack variations under normal conditions. The size of data payload is 512 bytes. This simulation, considers 200 sensor nodes. Nodes 11-200 are simple sensor nodes, and nodes 1 to 10 are the malicious nodes. Table 1 is the simulation parameters. Table 2 is the obtained mean values of network performance under no attack, black hole attack and rushing attack. The number of malicious nodes was varied from 2 to 10 and the results are compared with previous work [3]. The network performance is evaluated using packet delivery ratio (PDR), network throughput (NTh), packet drop ratio (PDrR), end to end delay (EED) and energy loss metrics in the presence of black hole and rushing attack.

Table 1. Simulation Parameters

Examined Protocol	GMR	Transmission range	250m
Simulator	NS-2	Movement model	Static
Simulation time	250 Seconds	Initial energy	5J
Simulation area	1000m x 1000m	RxPower	1.75mW
Number of sensor nodes	200	TxPower	1.75mW
Number of base stations	1	SensePower	1.75mW
Number of malicious nodes	1-10	IdlePower	1.75uW

5.1 Performance Analysis

The performance of the network is studied by analyzing packet delivery ratio(PDR), network throughput(NTh), packet drop ratio(PDrR), end to end delay(EED) and energy loss.

5.2 Packet Delivery Ratio (PDR)

Packet Delivery Ratio 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 as given in equation (4). Figure 7 represents the packet delivery ratio measured for the GMR protocol. The packet delivery ratio dramatically decreases in the presence of malicious node in the network. The mean packet delivery ratio is 80% when there is no attack. Due to the black hole attack, the mean packet delivery ratio decreases to 53 %. In case of rushing attack, the mean PDR decreases to 69% because of fast message forwarding.

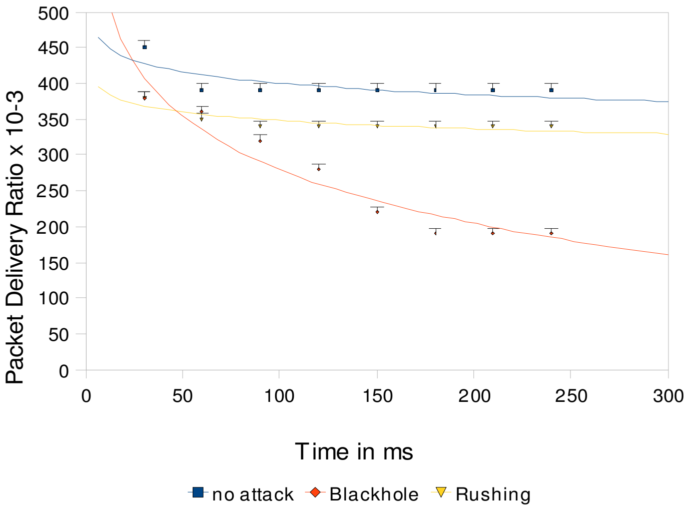

Figure 7. Packet Delivery Ratio

$$\text{Packet Delivery Ratio (PDR)} \quad = \quad \frac{\sum \text{of packets received by the destination node}}{\sum \text{of packets sent by the source node}} \qquad (4)$$

$$\text{Network Throughput (NTh)} \quad = \quad \frac{\sum \text{of packets generated by source node}}{\sum \text{of packets received at the destination}} \qquad (5)$$

$$\text{Packet Drop Ratio (PDrR)} \quad = \quad \frac{\sum \text{of packets dropped by the network}}{\sum \text{of packets generated by the network}} \qquad (6)$$

5.3 Network Throughput (NTh)

The network throughput (NTh) represents the numbers of data packets generated by the source node to the number of data packets received in the destination as given in formula (5). In Figure 8, the mean throughput of the network is 67% when there is no attack. For rushing attack, the malicious agent is launched at 100 ms and floods data packets to all its neighbors. As a result, the mean throughput is reduced to 53%. In case of black hole attack, the malicious node which is activated at 100 ms starts dropping the packets. Hence, the throughput regularly drops by 10% and the mean throughput decreases to 42% for black hole attack. From Figure 8, the throughput is high in the absence of attack.

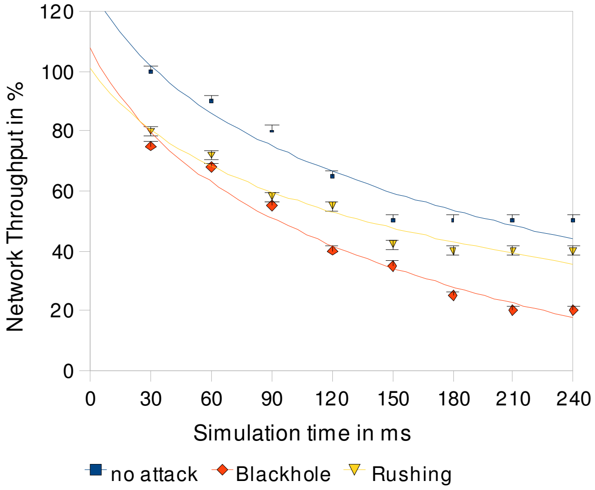

Figure 8. Network Throughput

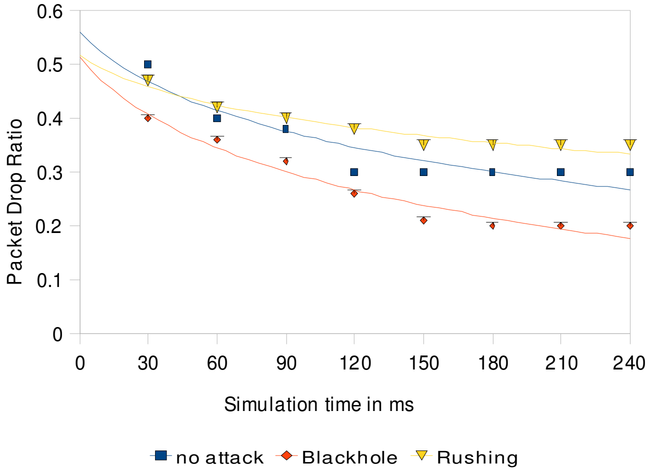

Figure 9. Packet Drop Ratio

5.4 Packet drop ratio (PDrR)

Packet drop ratio is the average number of packets dropped by the network to number of packets generated by the network as given in equation (6). Figure 9 is packet drop ratio in case of rushing and black hole attack. From Figure 9 for rushing attack, there is a packet loss between 50 ms to 120 ms because, the malicious node floods the data packets to all its neighbors in the next 70 ms. Rushing attack has a uniform packet loss after 120 ms. The packets dropped in the network is more for black hole than rushing attack.

Table 2. Mean values of Black hole attack and Rushing attack with 10 Malicious Nodes

Time	PDR	Network Throughput (%)	Packet Drop Ratio	End to End delay (Time)	Energy Loss (Joules)
NO ATTACK:					
30	450	100	0.5	3.8	4.3
60	390	90	0.4	3.8	4
90	390	80	0.38	3.9	3.9
120	390	65	0.3	3.9	3.3
150	390	50	0.3	4.2	2.5
180	390	50	0.3	4.2	2.2
210	390	50	0.3	4.2	2
240	390	50	0.3	4.2	1.8
Mean	**397.5**	**66.88**	**0.35**	**4.025**	**3.05**
BLACK HOLE ATTACK:					
30	380	75	0.4	4.8	4
60	360	68	0.36	4.8	4.2
90	320	55	0.32	5	3.9
120	280	40	0.26	5	3.2
150	220	35	0.21	5	2
180	190	25	0.2	5.5	0.8
210	190	20	0.2	5.5	0.5
240	190	20	0.2	5.5	0.5
Mean	**266.3**	**42.25**	**0.27**	**5.138**	**2.25**
RUSHING ATTACK:					
30	380	80	0.47	4.5	4.3
60	350	72	0.42	4.5	4.2
90	340	58	0.4	4.6	3.8
120	340	55	0.38	4.8	3.1
150	340	42	0.35	5.2	2.3
180	340	40	0.35	5.2	1.8
210	340	40	0.35	5.2	1.5
240	340	40	0.35	5.2	1.5
Mean	**346.3**	**53.4**	**0.38**	**4.9**	**2.9**

From Figure 10 the energy loss is uniform in case of no attack. The network drops its energy by two joule form 60 ms to 150 ms for rushing attack. In the next 30 ms rushing attack lost one joule and black hole attack losses two joules in next 50 ms. At 210 ms of simulation, the energy loss drops to 0.5 joules because of sudden disappearance of black hole nodes.

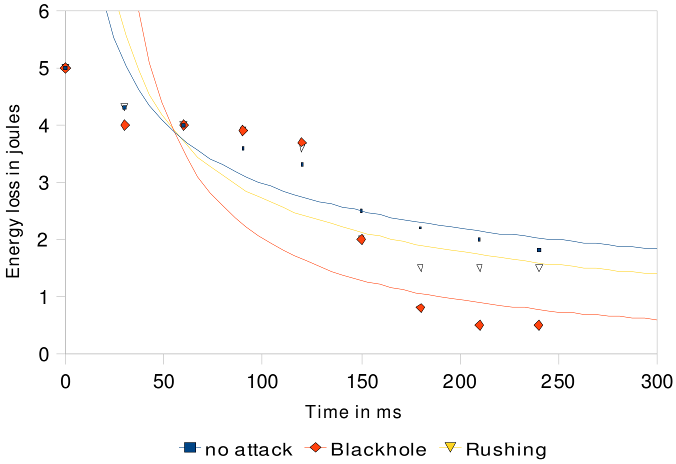

Figure 10. Energy Loss

5.5 MANET Vs WSN

Hoang et al have studied the rushing and black hole attack on a MANET mesh network with On Demand Multicast Routing Protocol (ODMRP). The average packet delivery ratio in this implementation is calculated by varying the malicious nodes from 2 to 10. The observations of this implementation are compared with the observations of Hoang et al[13]. From Figure 11 to 14, EW-R and EW-BH are the data values of rushing and black hole attack of Hoang et al. The OW-R and OW-BH represents the data values of rushing and black hole attack of this implementation. In WSN the rushing attack has 57% average PDR for two malicious nodes and if the malicious node increases to 10 nodes the PDR drops to 37%. But for MANET mesh network PDR drops to 20% for ten attackers. In case of black hole attack PDR varies from 47% to 18% in WSN. In case of MANET in the presence of black hole, the PDR is down to16%. Figure 12 shows the average network delay for MANET and WSN. The average network delay of rushing attack for WSN remains the same irrespective of the number of malicious nodes. For MANET delay is 40% in the presence of two malicious node and remains at 48% when the

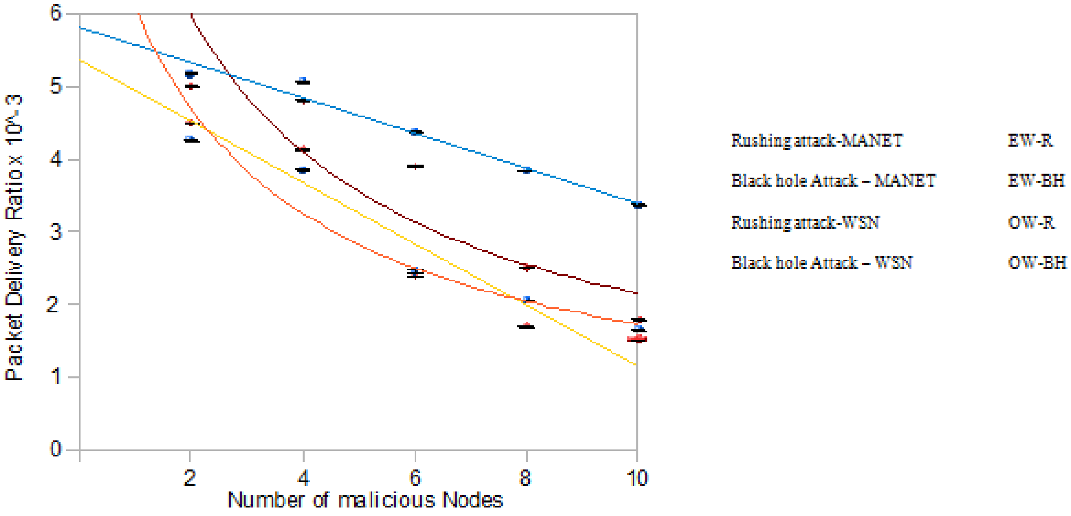

Figure 11. Comparison of Packet Delivery Ratio

number of malicious nodes is 8 and more. The black hole attack produces 61% and 52% delay for WSN and MANET respectively.

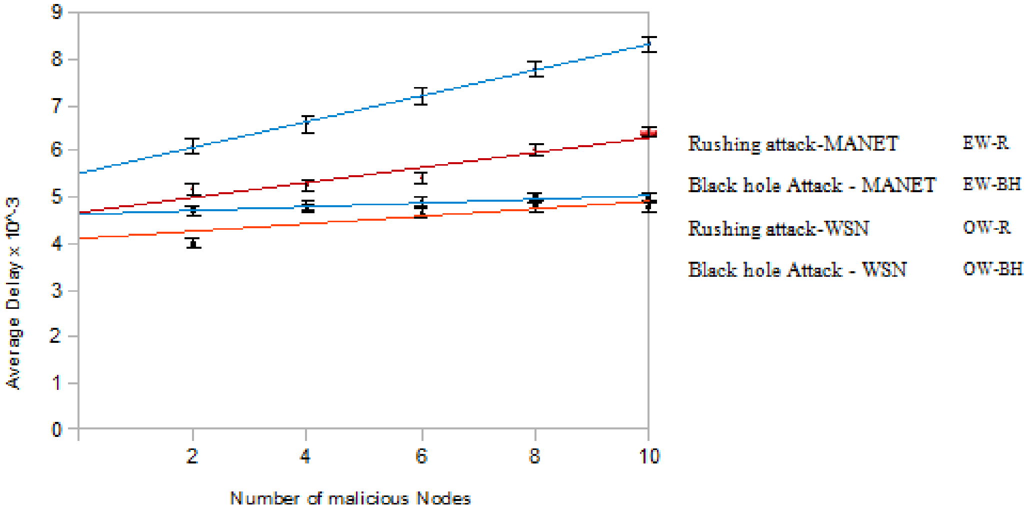

Figure 12. Comparison of Average Network Delay

Figure 13 is the average energy consumed by the rushing and black hole attack for the implemented WSN and the existing MANET. The battery power of sensor node is highly valuable resource which has to be used efficiently. For WSN the black hole node takes 89% of 5 joules and rushing attack consumes 35% of power. The black hole attack and replay attack for MANET takes 70% and 33% of total energy.

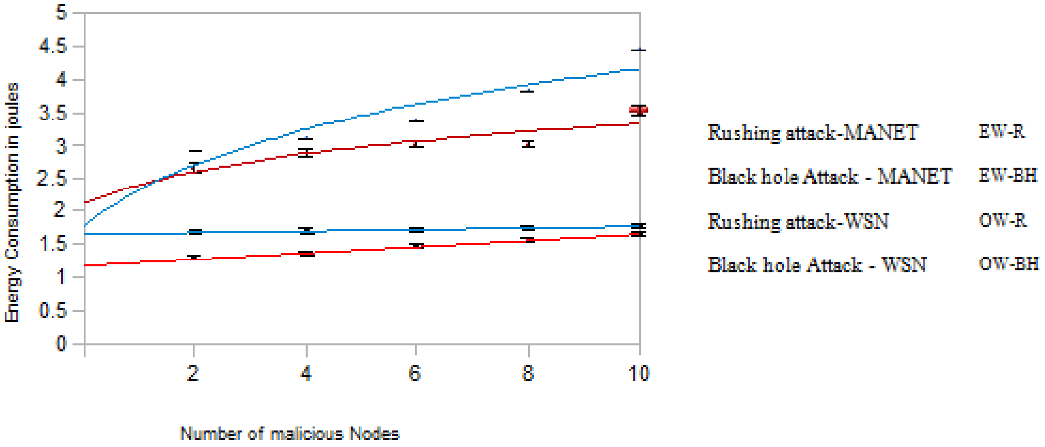

Figure 13. Comparison of Average Energy Consumption

Figure 14 shows the average energy loss of the network for varying number of malicious nodes. The average energy loss of the network is approximately same for WSN and MANET when the malicious node is two. When the strength of the malicious node increases to ten, the energy loss of the WSN and MANET for black hole attack is 84% and 89% respectively. The energy loss curve of the WSN is linear.

6. CONCLUSION

With the developments in WSN environments, the services based on WSN have increased. In this paper, the effect of black hole and rushing attack on GMR protocol has been studied. The packet delivery ratio, throughput, end-to-end delay and energy loss has been evaluated. There is reduction in packet delivery ratio, throughput and end to end delay as observed from the graphs. In black hole attack, all network traffics are redirected to a specific node or from the malicious node causing serious damage to GMR protocol. In rushing attack because of lengthier transmission queue in each node the performance of the network is degraded. From the performance metrics it is understood that the black hole is a severe routing attack for WSN. The behavior of rushing attack is almost same for WSN and MANET and affects the routing protocol.

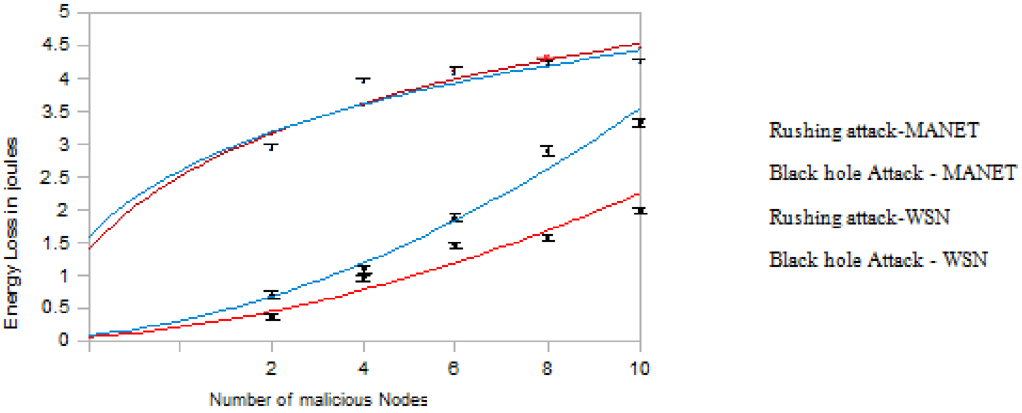

Figure 14. Comparison of Average Energy Loss

REFERENCES

[1] Anoosha Prathapani, Lakshmi Santhanam & Dharma P. Agrawal, (2010) "Detection of blackhole attack in a Wireless Mesh Network using intelligent honeypot agents", The Journal of Supercomputing (Online).

[2] Avinash Krishnan, Aishwarya Manjunath & Geetha J. Reddy, (2011) "Retracted: A New Protocol to Secure AODV in Mobile Ad-hoc Networks", Communications in Computer and Information Science, Vol. 133, No.5, pp 378-389.

[3] Eric Sabbah & Kyoung-Don Kang, (2009) "Security in Wireless Sensor Networks Computer Communications and Networks", Guide to Wireless Sensor Networks, First Edition pp. 491-512.

[4] Guoxing Zhan, Weisong Shi & Julia Deng, (2010) "TARF: A Trust-Aware Routing Framework for Wireless Sensor Networks," IEEE Transaction on Dependable and Secure Computing, Vol.9, No.2, pp. 184-197.

[5] Hoang Lan Nguyen & Uyen Trang Nguyen, (2008) "A study of different types of attacks on multicast in mobile ad hoc networks", Journal on Ad Hoc Networks", Vol.6, No. 1, pp.32-46.

[6] Jorge Hortelano, Carlos T. Calafate, Juan Carlos Cano, Massimiliano de Leoni & Pietro Manzoni, (2010), "Black-Hole Attacks in P2P Mobile Networks Discovered through Bayesian Filters" Lecture Notes in Computer Science, Vol. 6428, pp. 543-552.

[7] Kai Lin, Chin-Feng Lai, Xingang Liu & Xin Guan (2010), "Energy Efficiency Routing with Node Compromised Resistance in Wireless Sensor Networks", Mobile Networks and Applications (Online).

[8] Kai Xing, Shyaam Sundhar Rajamadam Srinivasan, Major Jose “Manny” Rivera, Jiang Li & Xiuzhen Cheng. (2010) “Attacks and Countermeasures in Sensor Networks: A Survey”, Network Security, pp. 251-272.

[9] Lianming Xu, Zhongliang Deng, Weizheng Ren & Hui Wang Sch (2008), “A Location Algorithm Integrating GPS and WSN in Pervasive Computing”, In Proceedings of Pervasive Computing and Applications, pp.461-466.

[10] NS-2: http://www.isi.edu/nnam/ns/.

[11] Phounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto & Nei Kato (2007), “A Survey of Routing Attacks In Mobile Ad Hoc Networks”, IEEE Wireless Communications, Vol.14, pp.85-91.

[12] Sanchez, J.A. Ruiz & P.M. Stojmnenovic (2007), “GMR: Geographic Multicast Routing for Wireless Sensor Networks”, Journal on Computer Communications, Vol. 30, No. 13, pp.2519-2531.

[13] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour & Yoshiaki Nemoto, (2007), “Detecting Black hole Attack on AODV based Mobile Ad-hoc networks by Dynamic Learning Method”, International Journal of Network Security, Vol. 5, pp.338– 346.

[14] SensorSim: NRL's Sensor Network Extension to NS-2, Naval Research Laboratory.

[15] Shyamala R and S.Valli (2009), “Secure route discovery in MAODV for Wireless Sensor Networks”, UbiCC Journal, Vol. 4, No. 3, pp.775-783.

[16] Shyamala Ramachandran and Valli Shanmugan, (2011) “Impact of Sybil and Wormhole Attacks in Location Based Geographic Multicast Routing Protocol for Wireless Sensor Networks”, Journal of Computer Science, Vol. 7 No.7, pp.973-979.

Authors

Shyamala Ramachandran received her B.E. in computer science from Madras University Chennai, Tamil Nadu, India in 1997 and M.E. degree in computer science and engineering from the Sathyamaba University Chennai, Tamil Nadu, India in 2002. At present, She is a part time research scholar in the Department Computer Science and Engineering, Anna University Chennai. Her research interests include wireless sensor networks and security.

Valli Shanmugam received her B.E. and M.E. degree in computer science and engineering from the Government College of Technology, Coimbatore, Tamil Nadu, India in 1990, and December, 1991, respectively. She got her Ph.D degree from the Department of Computer Science and Engineering, College of Engineering, Guindy, Anna University, Chennai, India in 2000. Her research interests include compilers, software engineering and security.