Middle-East Journal of Scientific Research 24 (12): 3696-3705, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.3696.3705

An Enhanced Study on the Simulation of Selfish Behavior Attack and Black Hole Attack on the Performance of Mobile AD HOC Network

[1]K. Rama Abirami and [2]M.G. Sumithra

[1]Department of Computer Science & Engineering,
PSNA College of Engineering and Technology, Dindigul, India
[2]Department of Electronics & Communication Engineering,
Bannari Amman Institute of Technology, Erode, India

Abstract: Mobile Ad hoc Networks (MANETs) are a self configuring wireless networks which consists of dynamic mobile nodes. Due to the infrastructure-less characteristic, MANETs are extremely subjected to several attacks. MANET nodes exchange information using the multi-hop wireless communications by routing protocols. Routing protocols are designed with an assumption that the nodes will cooperate in routing process. It is a cooperation based network that expects each participating node to forward packets to and from the destination. Selfish nodes are the defective nodes which drop the packets that are not intended to them. A node can act maliciously or selfishly and could harm the packet under transit. The objective of malicious and selfish behavior node is to disrupt communication and conserve own resources, respectively. Resource conservation by selfish nodes would also ultimately degrade the overall network performance. The open structure and limited battery-based energy in MANETs makes some nodes not to cooperate correctly or to behave maliciously which affects the fairness, reliability and efficiency. In this paper, certain attacks are modeled and simulated in NS2 network simulator by modifying the AODV routing agent. This paper presents the implementation details and some of the results of the evaluation.

Key words: MANET · Selfish behavior · Black hole attack · Routing protocols · AODV and Security

INTRODUCTION

In the recent years MANET has drawn the interest of researchers and commercial developers with its wide applications. MANET nodes does not have a prior knowledge about the nodes in the network and hence it works by trust and reputation system which plays an important role in the functioning of the various services such as service provision, access control and other collaboration in an open environment [1]. One of the security issues in MANET is non cooperation of the nodes in the network which arises in an attempt to save battery power and hence the nodes will be selfish in not forwarding the packets to the neighbor nodes. The nodes always behave rationally and hence it is very difficult to identify in the network [2]. Black hole attack is another one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. It is an analogy to the black hole in the universe in which things disappear. The node presents itself in such a way to the node that it can attract other nodes and networks knowing that it has the shortest path. MANET must have a secure way for transmission and communication which is quite challenging and vital issue [3]. Example for selfish behavior is as follows, Fig. 1. shows a MANET with nine nodes, if node 1 wants to send a packet to node 9, there are several possible paths to the destination with an assumption that all of the nodes are cooperative. If node 4 and 6 were non- cooperative nodes showing totally selfish behaviors, then all data from Node 1 must go through Node 3 (1-3-5-8-9) or through Node 5 (1-5-8-9), which is shown in Fig. 2.

Categories of Selfish Node Behaviors: Selfish nodes gains profits from the network as well as these nodes will preserve their own resources like bandwidth, battery life or hardware.

Corresponding Author: K. Rama Abirami, Department of Computer Science & Engineering,
PSNA College of Engineering and Technology, Dindigul, India.

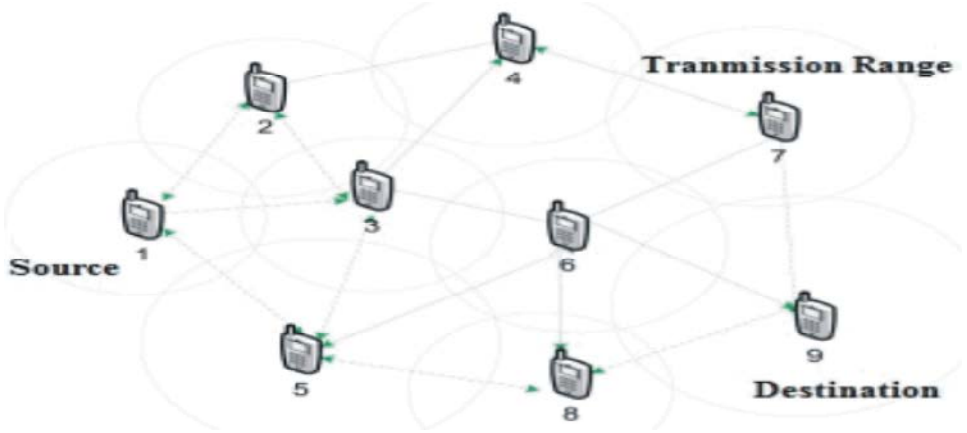

Fig. 1: MANETs with nine cooperative nodes

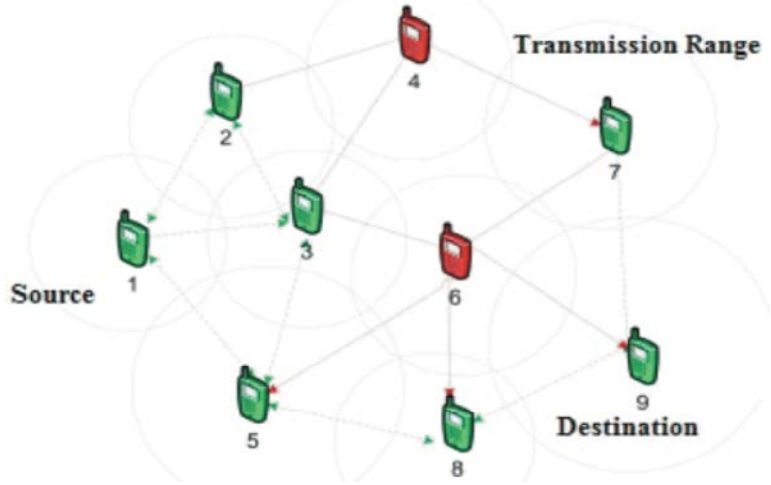

Fig. 2: MANET with two non cooperative nodes

The selfish node behaviors in AODV routing protocol are as follows [4]:

- Nodes which do not send Hello packet
- Nodes which do not send (Route Reply)RREP messages
- Nodes which do not forward data messages
- Nodes forwarding (Route Request) RREQ messages with delay
- Selfish behavior depending on the nodes energy

According to the routing, there are three types of selfish nodes:

Selfish Node Type 1 (SN1): These nodes involved in the (Dynamic Source Routing) DSR route discovery and Route maintenance phases, but deny to forward data packets.

Selfish Node Type 2 (SN2): These nodes do take part in neither the Route Discovery phase, nor forwarding data packets. They utilize their energy for transmission of their own packet.

Selfish Node Type 3 (SN3): Depending upon the energy level, these nodes behave or misbehave differently in the network. The nodes behave properly when the energy lies between full energy E and a threshold T1. The node will behave of type SN1 at the time the energy level is between T1 and another threshold T2. Finally, for an energy level lower than T2, it behaves like a node of type T2. The relationship between T1, T2 and E is T2<T1<E.

Selfish node behavior attacks are having different impact on performance and one particular type (the fully selfish node) cannot be detected. So in this work, first two types of selfish attack is simulated and left the third one which is the combination of first two types.

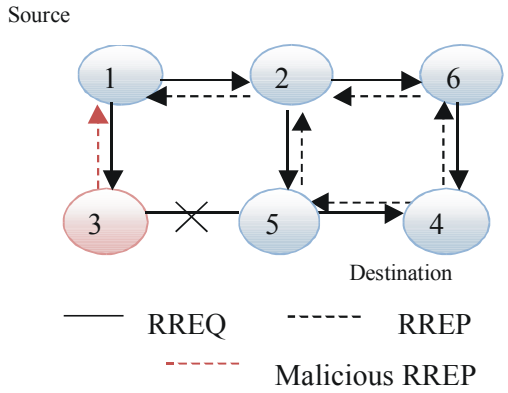

Fig. 3: Black Hole Attack

Black hole Attack: Black hole has more impact on proactive protocols like (Ad hoc On-Demand Distance Vector) AODV. It is a type of denial of service attack in which a malicious node sends false routing information, claiming that it has the finest route and diverts other nodes to forward data packets through malicious node. Thus consumes all the packets without forwarding them to the destination [5] which is shown in Fig. 3. There are two types of black hole attack in AODV. They are as follows [6].

Internal Black Hole Attack in AODV: An internal malicious node lies between the source and destination; once it gets the chance this malicious node make itself an active route for data forward. This type of attack is more dangerous to defend because it is difficult to detect the internal misbehaving node.

External Black Hole Attack in AODV: In External attacks, the nodes which stay outside of the network take the whole control of the network with the internal malicious node and disrupt the entire network.

Related Works: Recently, research work focused on selfish node behavior and black hole attack. Several related issues are briefly presented here:

Jeba kumar M. *et al.* [7] proposed a Token-based umpiring technique (TBUT) to detect and eliminate the selfish nodes effectively in MANET. There are two mechanisms in this method namely: packet dropping and a selfish node quarantining mechanism. The selfish node is traced and identified in packet dropping detection mechanism. After detection, the offending nodes are marked and eliminated from the network using selfish node quarantining mechanism.

Buttayan *et al.* [8] proposed an approach which introduced a virtual currency called Nuglets (also called as *beans*). This Nuglets is earned by forwarding the packets in the network. The security of the currency requires a trusted hardware which is the drawbacks of this approach.

Mart *et al.* [9] proposed a system which uses a watch dog that monitors the neighboring nodes to check whether they transmit the data further along the route. Consequently a misbehaving node is identified easily and avoids the routes with the component called pathrater. There are numbers of drawbacks such as selfish nodes are not identifies as misbehaving. The paths selected are excluded from the service.

Another system is the Collaborative Reputation Mechanism or CORE [10, 11]. In this approach each node collect the reputation values of their neighbor nodes and based on the ratings the nodes are allowed to take part in the network or are disqualified. A similar approach is conducted by Buchegger et al with the CONFIDENT system [12, 13]. Though, they only describe their detection mechanism and rely mostly on promiscuous overhearing.

An Acknowledgement based approach called 2 ACK scheme was proposed by Liu K *et al*. [14]. The main aim of this scheme is that, on the successful transmission of data packets over the next hop, the destination node of the next hop link will send back a special two hop acknowledgement called 2 ACK to indicate the successful receiving of the data packets. This scheme is a network-layer technique to detect misbehaving links and to mitigate their effects. Basic drawbacks of 2 ACK scheme is it cannot identify the specific node is selfish node. In the misbehaving links, the normal nodes also included and cannot be further used in the network and this leads to traffic congestion on the network.

Sun B *et al.* [15] proposed a neighborhood-based method to detect the black hole attack and a routing recovery protocol to build the correct path. Modify_Route_Entry control packet is sent by the source node to destination to renew routing path and also unconfirmed nodes are identified. Routing control overhead is reduced in this scheme. The disadvantage of this scheme is that the attackers cooperate to forge the reply packets.

Mohammad Al-Shurman et al proposed a Redundant Route Method and Unique Sequence Number Scheme [16] to avoid the black hole attacks in MANET. The foremost solution is to find multiple routes from the source to

destination node. The source node sends a ping packet, a RREQ packet, to the destination. The receiver will respond to the packet and the source node will examine the acknowledgement. In the next solution, a unique sequence value is accumulated which is higher than the current sequence number. Tables are maintained for last packet sequence number and the last packet received. Upon examining these tables, the sender node can identify the malicious node. Anyhow, these two mechanisms can be easily broke by two collaborative black hole nodes and hence it can withstand for black hole attack.

Satoshi *et al.* [17] proposed an AODV based dynamic learning system to detect black hole attack in MANET. A node along with the RREP packet, it checks if the sequence number is higher than the threshold value then it will be considered as malicious node. The threshold value will be dynamically updated periodically. The dynamic learning system improved the average end-to-end delay and normalized routing overhead. However, the detecting process will be complex, if a cooperative attack occurs in MANET. So, this solution is not suited for cooperative attacks.

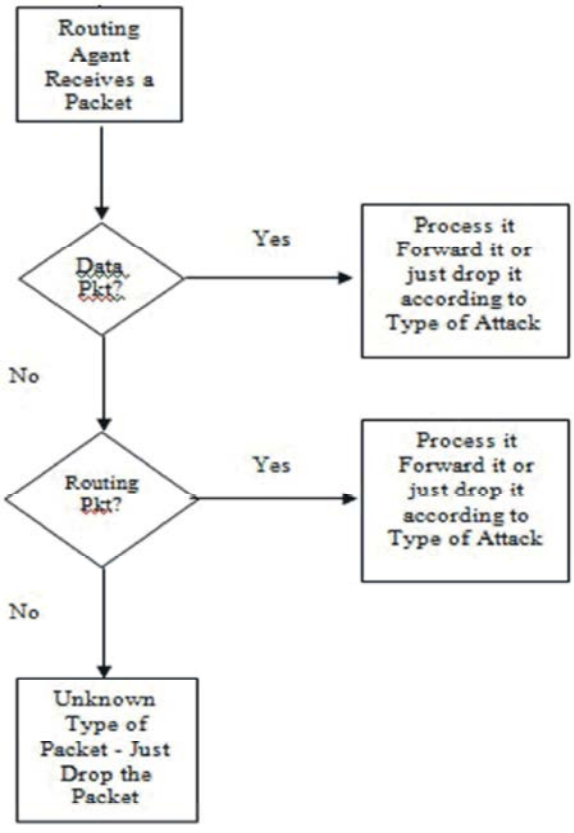

Fig. 4: Flow Diagram Shows AODV Receive Function

Djenouri D *at al*. [18] proposed a new method to monitor, detect and isolate black hole attack in MANET. A random two-hop ACK is employed in monitor phase. A local judgment approach uses Bayesian technique in detection phase. The method utilizes cooperatively witness-based verification, but it is difficult to prevent collaborative black hole attack as the judgment phase works in local side.

Most of the previous work gives a wrong idea that this kind of attack always lead to poor performance in terms of all the metrics. But it is not. In our work, the simulations are repeated for three times and only the average performance is taken into account.

Design of Attacks in Routing Layer: The flow diagram of the implementation of attacks in the routing layer is depicted in Figure 3.

Upon receiving the packet it checks for data packet or routing packet. If it is a data or routing packet, it will either process it or drop it according to the type of attack. If it is an unknown packet, it will drop the packet (pkt).

Experiment Performance Parameters

Simulation Parameters: The selfish behavior and black hole attacks are simulated on AODV protocol using NS2 simulator. The parameters used in the simulation are shown in Table 2. Random way point method was used for node mobility. The Common Node Parameters are shown in Table 1.

Evaluation Metrics: The performance of MANET routing protocols are evaluated using the following metrics:

Maliciously Dropped Packets: In this work, the no of packets which are dropped maliciously due to the attack are counted.

Packets Dropped at MAC Layer: The no of packets dropped at MAC layer which occur as a result of collision and other reason is considered as an important metric.

Packet Delivery Fraction/Ratio (PDF/PDR): PDF= ? Number of packet receive / ? Number of packet send.

Routing Load: Routing load is measured by the ratio of the number of routing messages generated (not forwarded) by the nodes in the network and the number of data packets successfully delivered to all the destination nodes.

Table 1: Common Node Parameters

Channel	Wireless Channel
Propagation	Two Ray Ground
Phy	Wireless Phy
Mac	802_11
Antenna	Omni Antenna
Link layer	LL
Queue	Drop Tail- PriQueue
Queue Length	50
Routing Protocol	AODV
Node-txPower	0.28183815
Node-rxPower	0.2819
Node-idlePower	0.14
Node Initial Energy	1000.0 Joules

(Note: rxPower and idlePower are intentionally set as high to simulate quick energy consumption)

Table 2: Traffic Parameters

Topography-X size	800m
Topography-Y size	800m
No. of Background Traffic Flows	10
Background Traffic Type	CBR (Constant Bit Rate)
Transport Agent	UDP
CBR-packet size	512bytes
CBR-interval	1 s
CBR-rate	10kb
Traffic Start Time	30th sec
Traffic Stop Time	100th sec

(Note: If No. of Malicious Nodes=0 and Type of Simulated Attack=Normal AODV, then it will simulate normal AODV routing protocol. Simulations are repeated for three times and only the average performance is taken into account, since it is enough to prove the impact of the attacks.)

End-End Delay: Average time in order to traverse the packet inside the network.

Overhead: Routing overhead is given by the total number of routing packets transmitted over the network, expressed in bits per second or packets per second.

Packets Dropped at Application Layer: It is the number of data packets that are not sent successfully to the destination, measured in numbers.

Throughput: Throughput gives the number of bytes or bits arrives at the sink over time and measured in kilo bits per second or mega bits per second.

MAC Load: It is the ratio of the number of MAC layer messages generated by every node and the number of data packets delivered successfully to the entire destination node.

Energy Consumption: It is the average of total energy consumed by all the nodes in the network, expressed in Joules.

RESULTS AND DISCUSSION

Results with Respect to Varying Number of Nodes: This section of results shows the performance of the simulation parameters by varying the no. of nodes as 30, 40 and 50.

Some of the Easily Interpretable Results: The following Fig. 5. and Fig. 6. shows the performance in terms of PDF and average of it. The black hole attack affected the PDF. The Selfish Behavior Type I also affected the PDF considerably. Selfish Behavior Type II does not affect the performance. So, both the Normal AODV without any attack and with the Selfish Behavior Type II attack performed almost equal.

The following Fig. 7 and Fig. 8. shows the performance in terms of dropped packets at application layer and average of it. The black hole attack induced packet dropping at application layer. The Selfish Behavior Type I also induced packet dropping at application layer considerably. Selfish Behavior Type II does not affect the performance. So, both the Normal AODV without any attack and with the Selfish Behavior Type II attack performed almost equal.

The following Fig. 9. and Fig. 10. shows the performance in terms of dropped packets at routing layer and average of it. The black hole attack induced packet dropping at routing layer. The Selfish Behavior Type I and Selfish Behavior Type II also induced packet dropping at routing layer considerably. By default, Normal AODV did not drop any packet maliciously at routing layer.

Results with Respect to Different Number of Malicious Nodes: This section of results shows the performance with respect to different number of malicious nodes. In this case, the number of malicious nodes is kept as 10.

Some of the Easily Interpretable Results: The following Fig. 11. and Fig. 12. Shows the performance in terms of PDF and average of it. The black hole attack affected the PDF. The Selfish Behavior Type I also affected the PDF considerably. Selfish Behavior Type II does not affect the performance.

The following Fig. 13. and Fig.14. shows the performance in terms of dropped packets at application layer and average of it. The black hole attack induced packet dropping at application layer. The Selfish Behavior Type I also induced packet dropping at application layer considerably. Selfish Behavior Type II does not affect the performance.

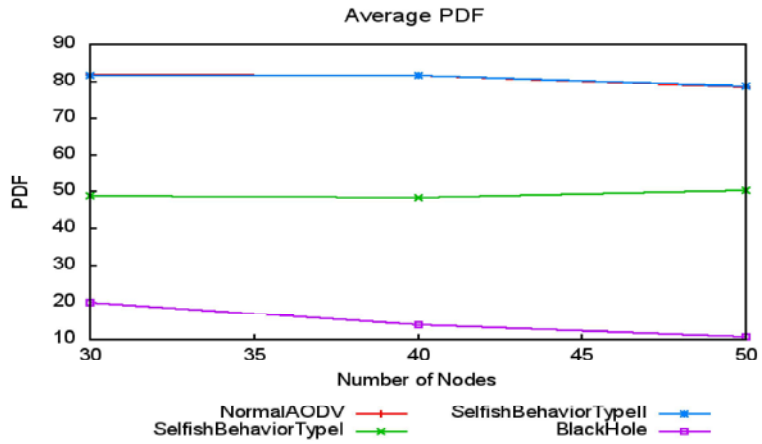

Fig. 5: Performance in PDF

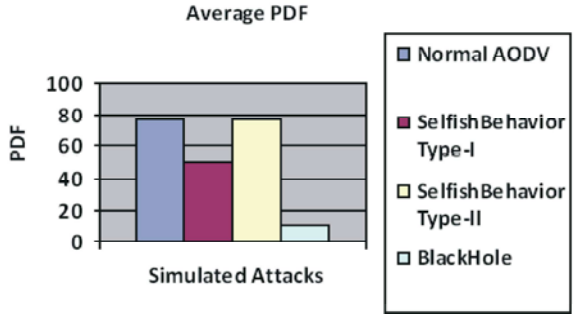

Fig. 6: The Average PDF

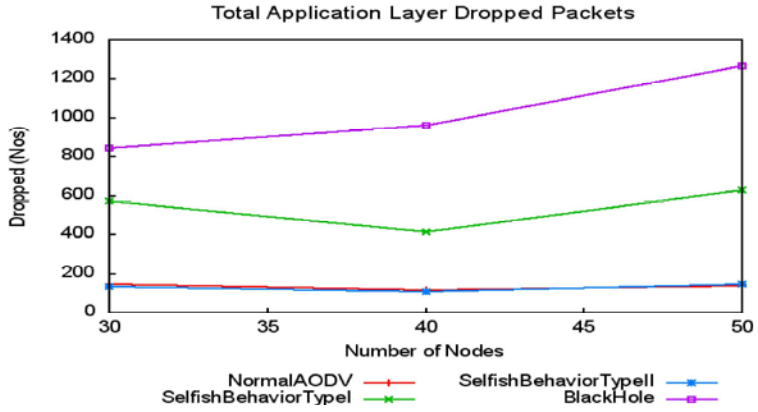

Fig. 7: Performance in Dropped Packets at Application Layer

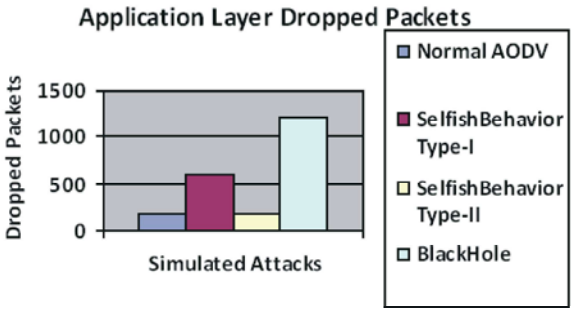

Fig. 8: The Average Dropped Packets at Application Layer

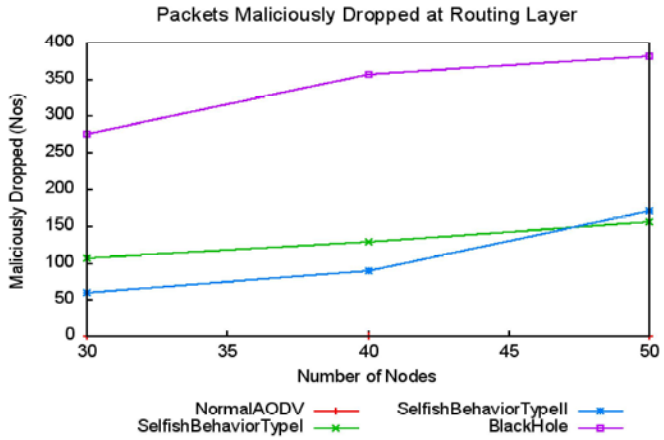

Fig. 9: Performance in Dropped Packets at Routing Layer

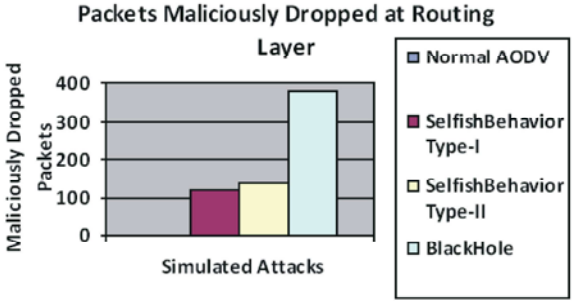

Fig. 10: The Average Maliciously Dropped Packets at Routing Layer

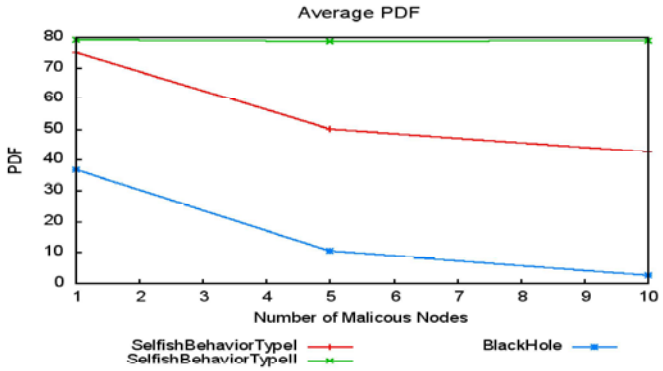

Fig. 11: Performance in PDF

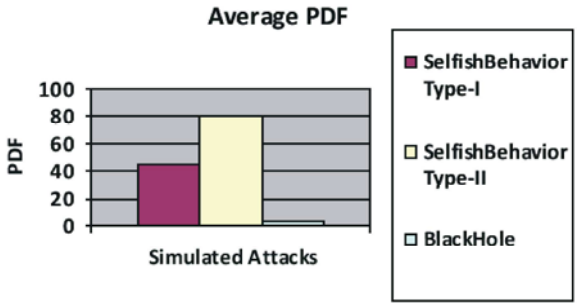

Fig. 12: The Average PDF

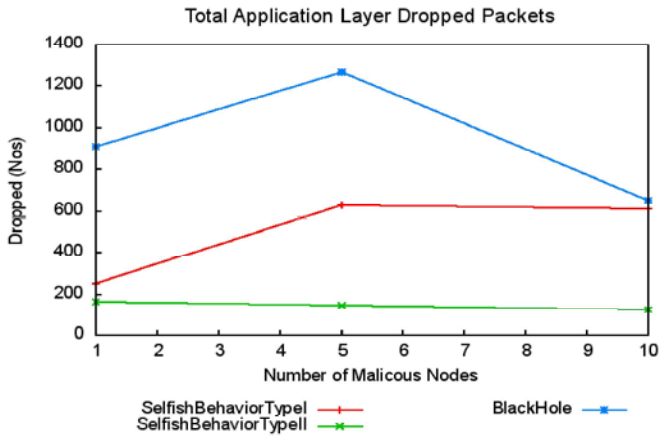

Fig. 13: Performance in Dropped Packets at Application Layer

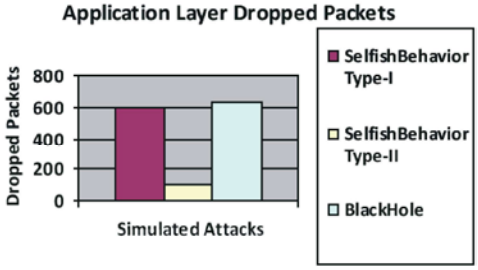

Fig. 14: Average Dropped Packets at Application Layer

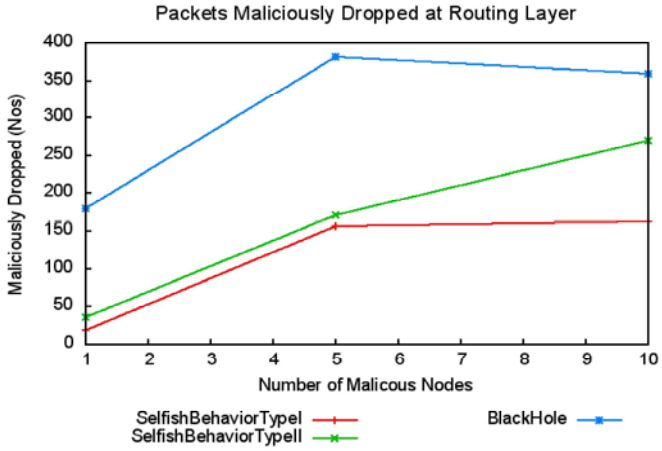

Fig. 15: Performance in Dropped Packets at Routing Layer

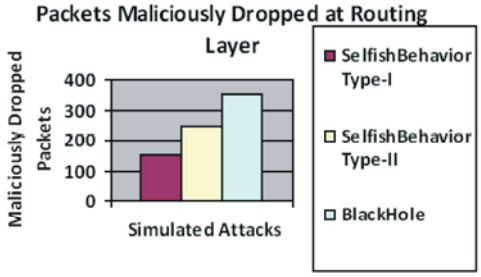

Fig. 16: The Average Dropped Packets at Routing Layer

The following Fig. 15 and Fig. 16 shows the performance in terms of dropped packets at routing layer and average of it. The black hole attack induced packet dropping at routing layer. The Selfish Behavior Type I and Selfish Behavior Type II also induced packet dropping at routing layer considerably.

CONCLUSION

Most of the evaluated metrics obviously prove the impact of selfish behaviors and black hole attack. The two types of selfish behaviors and the black hole attack affected the performance of MANET very much. With 10 malicious black hole nodes among the 50 nodes, the performance in terms of PDF is getting reduced. The results shows that, in a 50 node MANET, if there will be 10 malicious black hole nodes, then practically it is not possible to use the network for any reliable communication.

In this work, a light CBR traffic over UDP is used for evaluating the impact of these attacks. If TCP and much rapid traffic like FTP traffic are used, then the impact of the attacks will be very high. Future works may evaluate the performance while using TCP traffic. Future works may also address the efficient ways to detect and prevent these attacks.

REFERENCES

1. Al-Shurman, M., S.M. Yoo and S. Park, 2004. Black hole Attack in Mobile Ad Hoc Networks. Paper presented at the 42nd Annual ACM Southeast Regional Conference, Huntsville, Alabama, pp: 2-3.
2. Youngwan, Yoo and P. Dharma, 2006. Why Does it Pay to be Selfish in MANET?. IEEE Wireless Communications, pp: 87-97.
3. Fan-Hsun, Tseng, Li-Der, Chou and Han-Chieh, Chao, 2011. A Survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and information Sciences, pp: 1-4.
4. Tarag, F. and A. Robert, 2006. A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks. Liverpool John Moores University.
5. Jaspal Kumar, M., Kulkarni and Daya Gupta, 2013. Effect of Black hole Attack on MANET Routing Protocols. International Journal of Computer Network and Information Security, 5: 64-72.
6. Biswas, K. and M.D. Liaqat Ali, 2007. Security threats in Mobile Ad-Hoc Network. Master Thesis, Bleking Institute of Technology, Sweden.
7. Jeba Kumar, M., A. Kathirvel and N. Kirubakaran, 2015. A Unified Approach for detecting and eliminating selfish nodes in MANETs using TBUT. EURASIP Journal on Wireless Communications and Networking, pp: 143.
8. Buttayan, L. and J.P. Hubaux, 2003. Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks. ACM/Kluwer Mobile Networks and Applications, pp: 8.
9. Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks. Mobile Computing and Networking, pp: 255-265.
10. Michiardi, P. and R. Molva, 2002. CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. Presented at Communication and Multimedia Security, Portoroz, Solvenia.
11. Michiardi, P. and R. Molva, 2002. Preventing denial of service and selfishness in ad hoc networks. Presented at Working Session on Security in Ad Hoc Networks, Lausanne, Switzerland.
12. Buchegger, S. and J.Y.L. Boudec, 2002. Performance Analysis of the CONFIDENT PROTOCOL: Coperation of Nodes- Fairness in Distributed Ad-Hoc Networks. Presented at IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne.
13. Buchegger, S. and J.Y.L. Boudec, 2002. Nodes Bearing Grudges: Towards Routing Security, Fairness and Robustness in Mobile Ad hoc Networks. Presented at Tenth Euromicro Workshop on Parallel, distributed and Network based Processing, Canary Islands, Spain.
14. Liu K., J. Deng, P.K. Varshney and K. Balakrishnan 2007. An Acknowledgement-based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Transactions on Mobile Computing, 6(5): 536-550.
15. Sun, B., Y. Guan, J. Chen and U.W. Pooch, 2003. Detecting Black hole Attack in Mobile Ad Hoc Networks. Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, pp: 22-25.
16. Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Ne, Oto and Nei Kato Tohoku University, Abbas Jamalipou, University of Sydney, (2007). A Survey of Routing attacks in Mobile Ad Hoc Networks. IEEE wireless Communications, pp: 85-91.

17. Satoshi, K., N. Hidehisa, K. Nei, J. Abbas and N. Yoshiaki, 2007. Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method. International Journal of Network Security, 5(3): 338-346.

18. Djenouri, D. and N. Badache, 2008. Struggling Against Selfishness and Black Hole Attacks in MANETs. Wireless Communications & Mobile Computing, 8(6): 689-704.