Analyzing Misbehavior of Selfish Nodes in Mobile Adhoc Network

Pragya Singhal
Dept of IT, PIET, Samalkha, Haryana

Rakesh Kumar
Dept of IT, MMU, Mullana, Haryana

ABSTRACT

In Mobile Adhoc Networks (MANET), various types of Denial of Service Attacks (DoS) are possible because of the inherent limitations of its routing protocols. MANET rely on cooperation of all participating nodes, thus they are vulnerable to selfish nodes. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish or misbehaving nodes. These selfish nodes may severely affect the performance of network. Selfish node attack is a kind of Passive attack. In this paper misbehavior of Selfish Nodes is evaluated by finding the packet delivery ratio, energy consumption, end to end delivery and collisions by varying node mobility and number of attackers. Misbehaving nodes presence is one major security threat in MANET that can affect the performance of the under-lying protocols. Experiments are performed by implementing this through simulation using Glomosim Simulator and use AODV routing protocol. Results show that this drops the network performance.

Keywords: AODV, DoS, Glomosim MANET, PDR, Routing, etc.

1. INTRODUCTION

Adhoc networks are wireless networks where nodes communicate with each other using multi-hop links. There is no stationary infrastructure or base station for communication. Each node itself acts as a router for forwarding and receiving packets to/from other nodes.

A MANET, sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links [1]. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger internet.

MANETs, also known as short-lived networks, are autonomous systems of mobile nodes forming network in the absence of any centralized support. This is a new form of network and might be able to provide services at places where it is not possible otherwise.

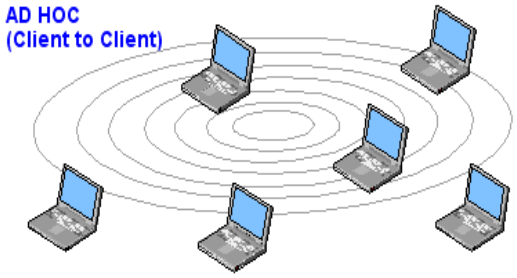

Figure 1: Mobile Adhoc Network.

MANETs have properties that increase their vulnerability to attacks. Constraints in bandwidth, computing power and battery power in mobile devices can lead to application-specific tradeoffs between security and resource consumption of the device. By diverting the traffic towards or away from a node, incorrect forwarding, no forwarding at all, or other non-cooperative behavior, nodes can attack the network. Nodes in MANETs do not have any central base station to coordinate the transmission and authentication of packets so the delivery of data packets from source to destination nodes in the network is dependent on the cooperation of the (intermediate) nodes in the network [2].

In MANETs various types of DoS are also possible because of the inherent limitations of its routing protocols. A DoS attack always attempts to stop the victim from serving legitimate users [3]. A DoS attack is a attack which relies on multiple compromised hosts in the network to attack the victim [14]. There are two types of DoS attacks i.e. passive and active DoS attacks. The First type of DoS attack has the aim of attacking the victim node in order to drop some or all of the data packets sent to it for further forwarding even when no congestion occurs, which is known as Passive DoS attack[10]. The second type of DoS attack is based on a huge volume of attack traffic, which is known as an Active DoS attack [4, 13]. One type of passive DoS attacks is selfish node attack in which node does not participate in network operation and it discard some or all of data packets sent to it without handling them properly even when no congestion occur [5]. Due to various new type of attacks security is becoming an important concept in MANET nowadays. The paper is divided into following sections. These are: i) Components of attack ii) Selfish node attack iii) Simulation iv) Experimental Result and Analysis v) Conclusion

2. COMPONENTS OF ATTACKS

Attack is composed of four elements, as shown below. First, it involves a victim, i.e., the target host that has been chosen to receive the brunt of the attack. Second, it involves the presence of the attack daemon agents. These are agent programs that actually conduct the attack on the target victim.

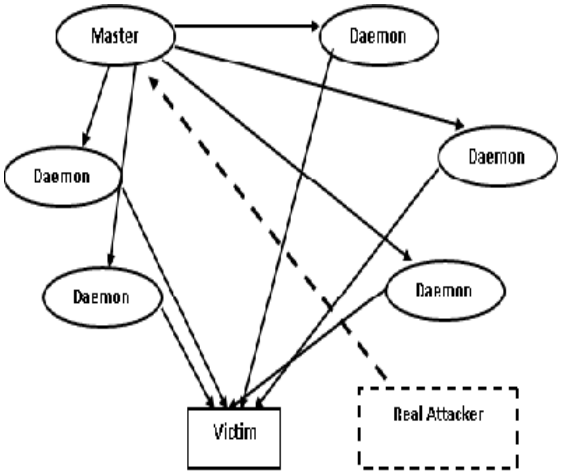

Figure 2: The Components of attacks [4]

Attack daemons are usually deployed in host computers. These daemons affect both the target and the host computers. The third component of a distributed denial of service attack is the control master program. Its task is to coordinate the attack. Finally, there is the real attacker, the mastermind behind the attack. By using a control master program, the real attacker can stay behind the scenes of the attack. The following steps take place during a distributed attack.

- The real attacker sends an "execute" message to the control master program.
- The control master program receives the "execute" message and propagates the command to the attack daemons under its control.
- Upon receiving the attack command, the attack daemons begin the attack on the victim.

3. SELFISH NODE ATTACK

MANETs rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET gets. But supporting a MANET is a cost-intensive activity for a mobile node. Detecting routes and forwarding packets consumes local CPU time, memory, network-bandwidth, and last but not least energy [7]. Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data. Some resources, namely battery power (energy), are scarce in a mobile environment and can be depleted at fast pace with the device utilization. This can lead to a selfish behavior of the device owner that may attempt to take the benefit from the resources provided by the other nodes without, in return, making available the resources of his own devices. In this scenario, open MANETs will likely resemble social environments. A group of persons can provide benefits to each of its members as long as everyone provides his contribution. For our particular case, each member of a MANET will be called to forward messages and to participate on routing protocols. A selfish behavior threatens the entire community. Optimal paths may not be available. As a response, other nodes may also start to behave in the same way.

3.1. Selfish Node Attack Mechanism

Selfish node attack presents a new threat to wireless ad hoc networks since they lack physical protection and strong access control mechanism. An adversary can easily join the network or capture a mobile node and then starts to disrupt network communication by silently dropping packets [11]. It is also a threat to the Internet since the various software vulnerabilities would allow attackers to gain remote control of routers on the Internet. If selfish node attack is used along with other attacking techniques, such as shorter distance fraud, it can create more powerful attacks i.e. black hole which may completely disrupt network communication.

Now let us illustrate selfish node with an example.

Suppose we want to send packets from node *S* to node *D* shown in the network. Shortest Path from node S to node D is:

$$S \rightarrow M \rightarrow G \rightarrow N \rightarrow D$$

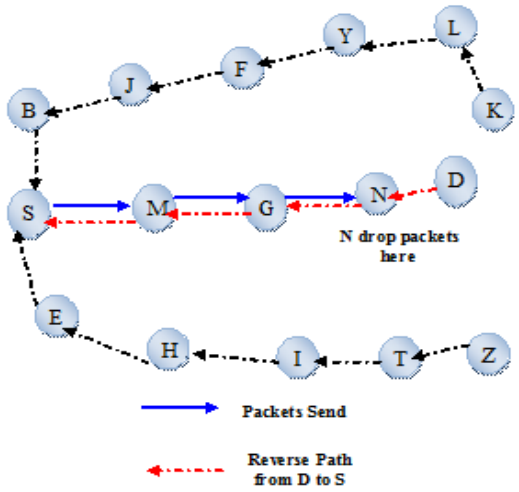

Figure 3: Selfish Node Attack

In case of selfish node attack, suppose node *N* becomes selfish and because of attack on node *N*, it does not forward the packets to node *D*. There is a path from node *S* to node *D*, and there is no congestion in the network, still node *D* does not receives the packet because of selfish node *N*.

3.2 Implementation of Selfish Node Attack

A selfish node can silently drop some or all of the data packets sent to it for further forwarding even when no congestion occurs. Selfish node attack presents a new threat to wireless ad hoc networks since they lack physical protection and strong access control mechanism. An adversary can easily join the network or capture a mobile node and then starts to disrupt network communication by silently dropping packets. Selfish node attack is a serious threat to the routing infrastructure of both MANET and the Internet since it is easy to launch and difficult to detect. To launch the attack, an attacker needs to gain the control of at least one router in the target network. The router used to launch the attack can be a specialized router or a computer running routing software. To gain access to a specialized router, an attacker can explore the software vulnerability of a router.

In this attack, the attacker makes some nodes malicious, and the malicious nodes drops some or all data packets sent to it for further forwarding even when no congestion occurs. Code for implementing selfish node attack is shown below

```
if((((node->nodeAddr)%2)==0)&&
(node->nodeAddr<= 14))
{
 return;
}
```

Here we are using GloMoSim simulator [15]. In this simulator we have a file name adov.pc for handling routing. This code is placed in different functions of aodv.pc file Code shown for packet dropping makes node 4, 6, 8, 10, 12 and 14 as malicious nodes. These nodes drop some or all data packets transmitted to it for further forwarding.

4. SIMULATION

Simulation is a fundamental tool in the development of MANET protocols, because the difficulty to deploy and debug them in real networks. Here we use glomosim simulator, Glomosim stands for Global Mobile information systems Simulation library [14].

The following quantitative metrics are to be used to evaluate the performance of the attacks in the mobile ad hoc network.

Packet Delivery Ratio (PDR): It is the ratio between the amount of incoming data packets and actually received data packets.

Number of Collisions: In a network, when two or more nodes attempt to transmit a packet across the network at the same time, a packet collision occurs. When a packet collision occurs, the packets are either discarded or sent back to their originating stations and then retransmitted in a timed sequence to avoid further collision.

Energy Consumption: Total energy consumed in the network is energy consumption. It is measured in mWhr.

End to End Delay: End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination. It is measured in second(s).

For our simulation procedure, we have been specific about certain parameters as mentioned below to enable hassle free simulation.

PARAMETER	VALUE
Number of Nodes	0-50
Terrain range	(1200,1200)
Bandwidth	2Mbps
Simulation Time	0 - 25 S
Node-placement	Uniform
Mobility	Random Waypoint Motion
Mobility	0 - 25 m/s
Traffic Model	CBR
MAC Protocol	CSMA
Routing Protocol	AODV
Pause Time	0

5. EXPERIMENTAL RESULT AND ANALYSIS

Effect of Selfish Node Attack Mechanism under Glomosim simulator is given below.

- **With Different Number of Attackers**

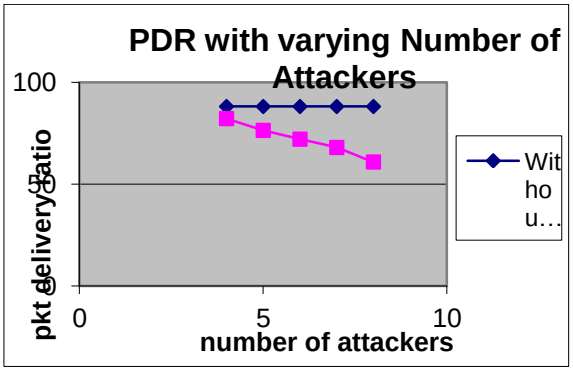

Figure 4: PDR with Varying number of Attackers

As shown in figure 4, the number of attackers per network is varied from 4 to 8. The PDR of the network decreases rapidly when it is subject to attacks. When the number of attacker is 0, the network performance does not seem to deteriorate significantly as traffic has not reached saturation point. However, as the number of attackers increases, there are more packets (both legitimate and illegitimate) which compete for channel access in the shared wireless medium. This leads to a drop in the packet delivery ratio.

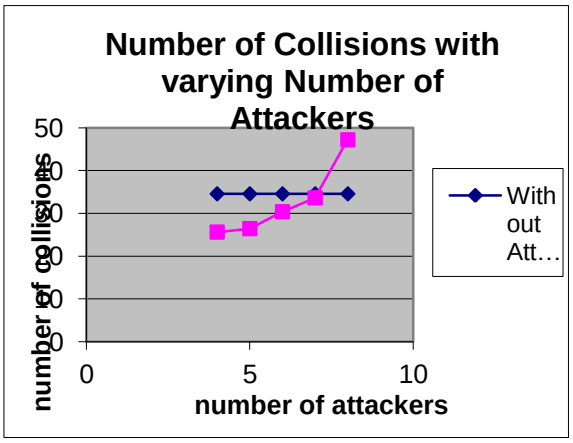

Figure 5: Number of Collisions with Varying number of Attackers

As shown in figure 5, the effect of selfish node attack on number of collisions per network with varying number of attackers. As the number of attackers increases, it causes increase in number of collisions i.e. packets are unable to reach at their destination. Thus, we can predict that as the number of attackers increases, the performance of the network will deteriorate even further.

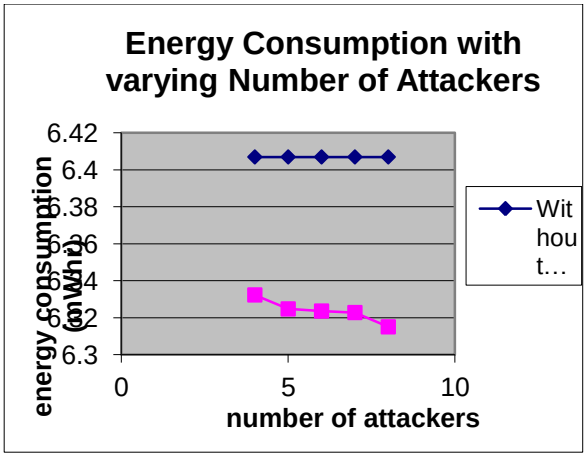

Figure 6: Energy Consumption with Varying number of Attackers

Figure 6 depicts the effect of selfish node attack on energy consumption with varying number of attackers. As the number of attackers increases energy consumption decreases because node behaving as selfish node because in selfish node attack node drops the packets send to it for further forwarding even when no congestion occur. Selfish node does not send packet to the destination node in order to save energy i.e. why energy decreases.

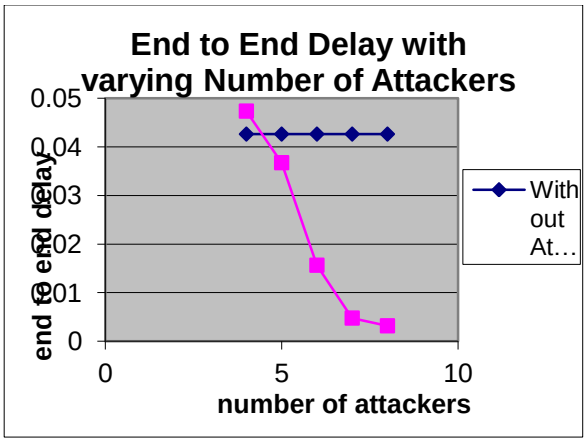

Figure 7: End to End Delay with Varying number of Attackers

Figure 7 shows the effect of selfish node attack on end to end delay with varying number of attackers. As the number of attackers increases, end to end delay decreases as shown in figure.

- **With Varying Node Mobility**

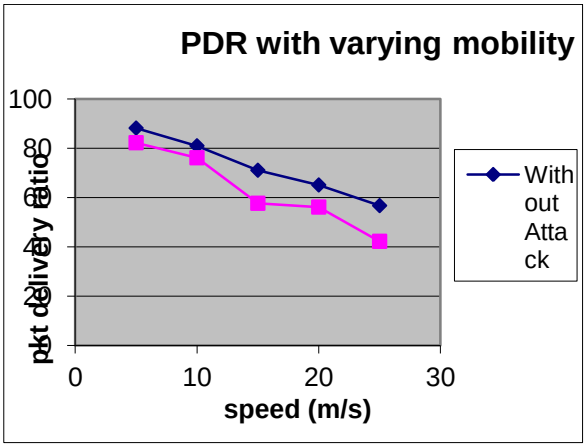

Figure 8: PDR with Varying Node Mobility

Figure 8 shows the effect of selfish node attack on PDR, when the speeds of the nodes are increased. As node mobility increases, link breakages occur more frequently and lead to route repairs and maintenance. This increases the overhead in the network, thus causing the network performance to deteriorate and packet delivery ratio (i.e. number of packets successfully transmitted) decreases. This shows the PDR when there is no attacker in the network and when number of attacker varies i.e. 3 with varying speeds of nodes. However, it is interesting to note that at low or no mobility, the performance of the network does not seem to deteriorate significantly. Therefore, static nodes or nodes with low mobilities may not be very much affected by selfish node attack (especially if traffic rate is low).

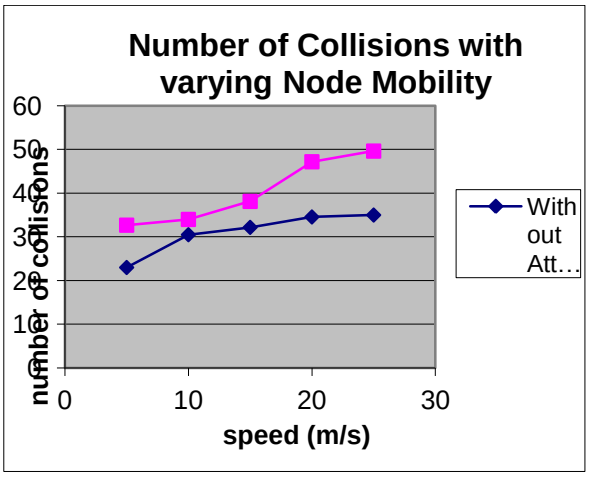

Figure 9: Number of Collisions with Varying Node Mobility

Figure 9 shows the effect of Selfish Node attack on number of collisions when speeds of nodes are increased. As the node mobility increases, link breakage occurs more frequently and this leads to the more collisions in the network. So, as the node mobility increases number of collisions also increases.

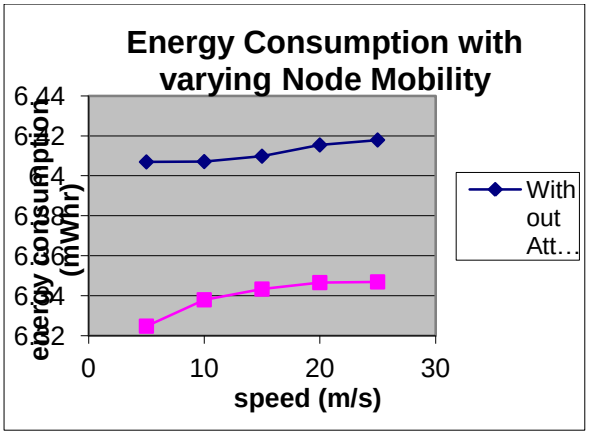

Figure 10: Energy Consumption with Varying Node Mobility

Figure 10 depicts the effect of Selfish Node on Energy Consumption when speeds of nodes are increased. As the node mobility increases, link breakage occurs more frequently, this leads to the more route repair and maintenance. So, more energy is consumed in route repair or to establish new path. Hence, as the node mobility increases energy consumption also increases.

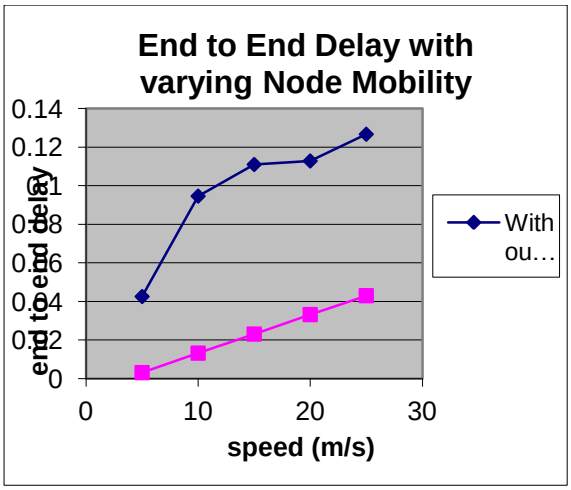

Figure11: End to End Delay with Varying Node Mobility

Figure 11 shows the effect of Selfish Node on End to End Delay when speeds of nodes are increased. As the node mobility increases, link breakage occurs more frequently, this leads to the more route repair and maintenance. So, end to end delay increases.

6. CONCLUSION

The mobile adhoc network suffers from several types of intrusions, out of which, the denial of service attack by a selfish node is the one of them. Misbehaving nodes presence is one major security threat in MANETs that can affect the performance of the under-lying protocols. Selfish node attack is a kind of Passive attack. In this paper, we have studied without attack and with selfish node attack impact on network performance when AODV routing protocol is used. Through simulations, we have seen how much selfish nodes can affect network performance. Simulation results brought up conclusion that network performance sharply drops when we compare the results. This paper describes the performance under AODV routing protocol ,in future other protocols are considered and also provides some prevention measure for these types of attacks.

7. REFERENCES

[1] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei (Department of Computer Science and Engineering) Florida Atlantic University, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", 2006 Springer.

[2] Geetha Jayakumar, and G. Gopinath, "Ad Hoc Mobile Wireless Networks Routing Protocols", Journal of Computer Science 3 (8), 2007, pp. 574-582.

[3] Sunil Taneja and Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010, pp. 279-285.

[4] Felix Lau , Stuart H. Rubin , Michael H. Smith, Lj ilj ana Traj koviC, "Distributed Denial of Service Attacks", June 2000, IEEE, pp. 2275-2280.

[5] G.S. Mamatha and Dr. S.C. Sharma, "Network Layer Attacks and Defense Mechanisms in MANETS- A Survey", International Journal of Computer Applications, Volume 9, No.9, November 2010, pp. 12-17.

[6] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad hoc on-demand distance vector (AODV) routing", RFC 3561, IETF; July 2003.

[7] T.V.P.Sundararajan, Dr.A.Shanmugam, "Performance Analysis of Selfish Node Aware Routing Protocol for Mobile Ad Hoc Networks", ICGST-CNIR Journal, Volume 9, Issue 1, July 2009.

[8] Sung-Ju Lee, Elizabeth M. Belding-Royer, Charles E. Perkins, "Ad hoc On-Demand Distance-Vector Routing Scalability", Mobile Computing and Communications Review, Volume 1, Number 2.

[9] Cong Hoan Vu, Adeyinka Soneye, "An Analysis of Collaborative Attacks on Mobile Ad hoc Networks", Thesis no: MCS-2009:4, June2009.

[10] Felix Lau, Stuart H. Rubin, Michael H. Smith and Ljiljana TrajkoviC; "Distributed Denial of Service Attacks"; 2004 IEEE; pp. 2275-2280

[11] Martin Schütte "Detecting Selfish and Malicious Nodes in MANETs" seminar: sicherheit in selbstorganisierenden netzen, hpi/universität potsdam, sommersemester 2006.

[12] Hong-Peng Wang, Lin Cui, "An Enhanced AODV for Mobile Ad Hoc Network", Proceedings of the Seventh International Conference on Machine Learning and Cybernetics, Kunming, 12-15 July 2008, IEEE.

[13] Stephen M. Specht and Ruby B. Lee; "Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures"; Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, September 2004; pp. 543-550.

[14] GloMoSim; Available on: http://pcl.cs.ucla.edu/projects/glomosim.

[15] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay; "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security (IJCSS), Volume (4), Issue (3), pp. 265-274.

[16] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad hoc on-demand distance vector (AODV) routing", RFC 3561, IETF; July 2003.