A Security Attacks On Dynamic Source Routing Protocol

Mr. Dhaval Kalaria
Post Graduate Student
Computer Engineering Department
Sri Balaji College of Engineering & Technology, Jaipur

Prof. Mrs. Saroj Hiranwal
Assistant Professor
Computer Engineering Department
Sri Balaji College of Engineering & Technology, Jaipur

***ABSTRACT*:** *Mobile Ad hoc NETwork (MANET) is a collection of wireless mobile nodes which may form a temporary network, without the use of any fixed infrastructure or centralized administration. Nodes rely on multi-hop routing protocols to forward data packets sent from a source node to a destination node which is out of its transmission range. Routing protocols are essential for a MANET in order to discover network topology and build routes, MANET routing protocols are designed to dynamically maintain routes between any pair of communicating nodes in spite of frequent topology changes caused by nodes' mobility. The problem of all the current ad hoc routing protocols is that they trust all nodes and assume that they behave properly; therefore they are vulnerable to attacks launched by misbehaving nodes. Nodes misbehave because they are malfunctioning, selfish or malicious. However, there is not a deep study of the impact of such attacks on the performance of routing protocols through simulations. So in this paper we have simulated attacks on DSR protocol and find out their effect on performance on basis various network parameters.*

Keywords— **Ad-Hoc Networks, Grey Hole attack, Selfish Behaviour, DSR, CBR Traffic.**

I. INTRODUCTION

A mobile ad hoc network is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time.

The basic characteristic of these networks is the complete lack of any kind of infrastructure, and therefore the absence of dedicated nodes that provide network management operations like the traditional routers in fixed networks. In order to maintain connectivity in a mobile ad hoc network all participating nodes have to perform routing of network traffic. The cooperation of nodes cannot be enforced by a centralized administration authority since one does not exist. Therefore, a network layer protocol designed for such self-organized networks must enforce connectivity and security requirements in order to guarantee the undisrupted operation of the higher layer protocols.

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension [2]. Because of this features, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks.

In section 2 ,we explore DSR protocol. Section 3 define and explain DoS attack. Section 4 say problem statement and analyze the performance of DSR through simulation result. Section 5 concludes the paper. Section 6 specify the future work.

II. DSR PROTOCOL OPERATION

There are two categories of routing protocol in Ad-Hoc network, Reactive and Proactive.[3] Protocols cab be proactive which means that nodes periodically registers changes in the topology and updates routing information. The routes are stored and maintained in routing tables. Proactive protocols have the advantage that there is little latency since routes are already available, but the disadvantage is that they require nodes to periodically update routing tables. The other approach is reactive protocols. Routes are discovered on demand, when data need to be transmitted to the node. Advantage of on demand routing is that it saves bandwidth by reducing routing overhead. Disadvantage is the latency at the beginning of transmission to nodes when no route, have yet been discovered.

Dynamic Source Routing (DSR) [3] is specifically designed for use in multi-hop wireless ad hoc networks. The protocol does not require any existing infrastructure or administration and is completely self-organizing and self configuring. DSR is source routing protocol, which means the entire route is known before transmission is begun. DSR stores discovered routes in Route Cache. The protocol basically consists of the two mechanisms:

- Route Discovery
- Route Maintenance

A. *Route Discovery*

When source node sends a packet to the destination node, it first searches its route cache for suitable route to destination. If no route from source to destination exists in source's route cache, Source initiates Route Discovery and sends out a ROUTE REQUEST message to find the route. The source node is referred to as initiator and destination node as the target. When a node receives a ROUTE REQUEST message it examine the target ID to determine if it is the target of message. If not, then nodes own id is appended to the address list and the RReq is broadcasted. If the the node is the target it returns a ROUTE REPLY message to the initiator. This ROUTE REPLY message includes the accumulated route from the ROUTE REQUEST message.

B. *Route Maintenance*

Since nodes move in and out of transmission range of other nodes and thereby creates and breaks routes, it is necessary to maintain the routes that are stored in the route cache. When a node receives a packet it is responsible for confirming that the packet reaches the next node on the route. Figure illustrates the mechanism work like a chain where each link has to make sure that the link in front of it not broken.

III. Security attacks on DSR protocol

The attacks on MANET are classified as passive attacks and active attacks. In passive attacks, an intruder snoops the data exchanged between the nodes without altering it. In these type of attacks, a selfish node abuses constrained resources such as battery power for its own benefit. The goal of an attacker is to obtain the information that is being transmitted that leads to the violation of massage confidentiality. Passive attacks are difficult to detect because the activity of the network is not disrupted in these attacks.

In active attacks, an attacker actively participates in disrupting the normal operation of the network services. A Denial of Service attack is one of active attack distributed in nature, large scale attempt by malicious users to disrupt connection between two machines, thereby preventing access to a service or to disrupt service to a specific system.[4] This exhausts the victim network of resources such as bandwidth, battery, computing power, etc. The victims are unable to provide services to its legitimate clients and network performance is greatly deteriorated.

One of the most important active attack is grey hole attack and passive attack is forwarding node selfish behavior. We need to find the effect of this attacks on DSR.

A. Grey Hole Malicious Attack

In this case, the attacker introduce itself as co-operating node, it participate in route request and route reply mechanism, it make sure that it will be available on the path. After the route discovery mechanism, when source node transmit data packet at that time malicious user just drop all the data packet. In other words, such attacker does not allow that all of packets arrive at real destination [4].

B. Forwarding Node Selfish Behavior

In this behavior, Selfish node disable packet forwarding function of dynamic source routing protocol. When this behavior is applied, the node disables the packet forwarding function for all packets that have a source address or destination address different from the current selfish node. Node with this kind of selfish behavior does not participate in route discovery phase of DSR protocol and does not forward any data packet. Node behave selfishly to save it resources like battery and bandwidth.

IV. Simulation Environment

We conducted exhaustive simulations in the simulation tool NS-2.34 [20] [21]. We took average of 10 simulations. The number of nodes (network size N) is 50. The mobility model chosen is the Random Way Point Model [18], which is general in nature and provides the uniform node distributions. Unless otherwise indicated, the speed is uniformly distributed between 0 and 20 ms. we used Random Way Point model [18] because we were not targeting particular application. Constant Bit Rate (CBR) traffic model is chosen for generating data packets.

The results are averaged of 10 simulation rounds conducted with various random seeds. The simulation time is set to 1000s so that the system can reach steady states. We set maximum number of packet as 10000 which is large enough to continue session till end of the simulation time. Other general parameter mentioned in table 1.

TABLE I
PARAMETERS USED IN NS-2 SIMULATOR

Simulation time	500 sec
Number of Nodes	50
Routing Protocol	DSR
Traffic	CBR
Packet Size	512 Bytes
Number of traces	10

Topologies	Dynamic
Mobility Model	Random Way Point

For the evaluation we use following metrics in our study:

1) Packet Delivery Ratio: The packet delivery ratio of a receiver is defined as the ratio of the number of data packets received by receiver over the number of data packets transmitted by the sender.

2) Throughput: Network throughput refers to the average data rate of successful data or message delivery over a specific communications link.

3) End to End Delay: The end to end delay of a packet is defined as the time a packet takes to travel from the source to destination.

4) Routing Overhead: Routing Overhead is defined as number of routing packets have been used in simulation.

V. SIMULATION RESULTS

Following are our simulation results that demonstrate the effects of grey hole attack and forwarding node selfish behavior on DSR protocol in Mobile Ad-Hoc Networks.

- **Grey Hole Attack Simulation Result**

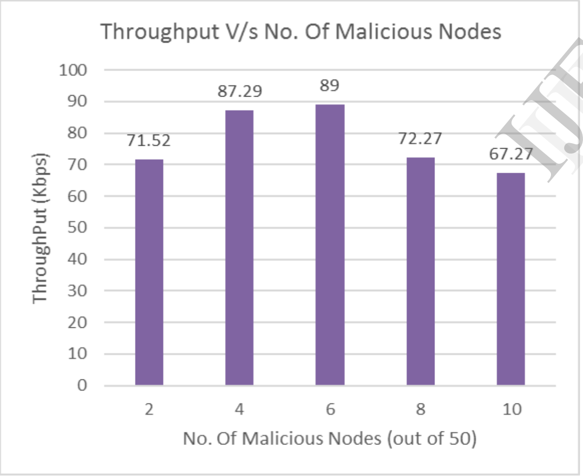


Figure 1. Throughput Analysis Grey Hole Attack

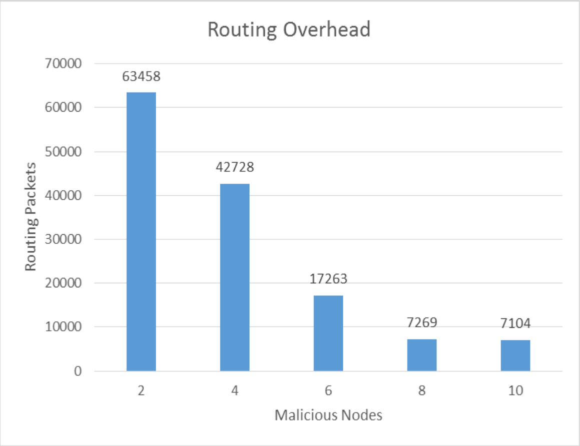
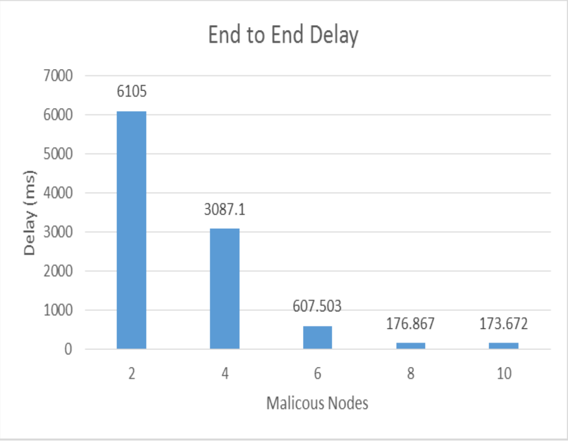


Figure 2. Routing Overhead Grey Hole Attack

Figure 3. End to End Delay Grey Hole Attack



Summary of Grey Hole Attack:

The performance of routing protocols in MANET depends heavily on much kind of attacks. One of these attacks is grey hole attack. The results of simulation shows that this attack has high effect on DSR protocol.

It is to be observed from figure 1 that as number of attackers are increasing in network, network throughput tend to decrease because malicious node tend to drop data packets. As data packets are dropped by malicious nodes, good node does not have any way to identify whether packet has been reached or not and believe that packets have been reached and they do not need to retransmit it. This characteristic intern reduce routing overhead as shown in figure 2 and end to end delay as shown in figure 3 of network.

- **Forwarding Node Selfish Misbehavior**

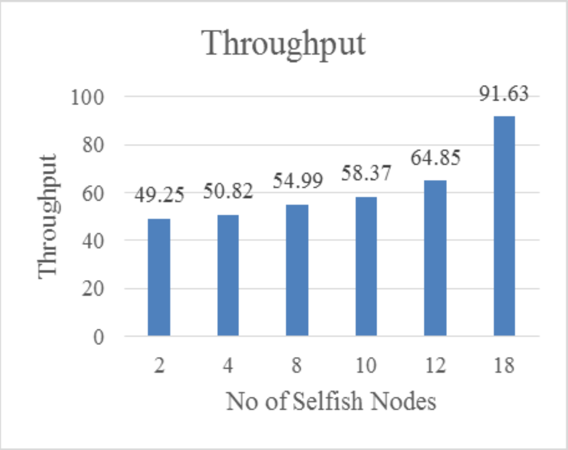


Figure 4. Throughput Forwarding Node Selfish Behaviour

Figure 4 shows the throughput of network with varying number of selfish nodes. As number of selfish nodes increases up to certain level, the network throughput increases due to reduction in number of collisions. We observe the decrease in throughput after the threshold point (more than twenty selfish nodes in network). This is due to the fact that as more and more nodes behave selfishly, network becomes partitioned and nodes face difficulty in establishing end to end path from source to destination.

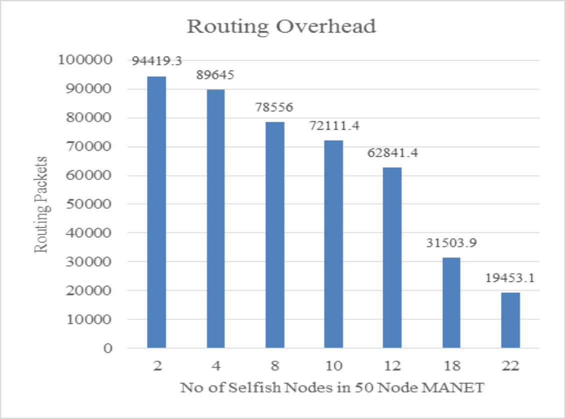


Figure 5. Routing Overhead Forwarding Node Selfish Behaviour

From Figure 5, we can say that when some nodes behave selfishly, they drop control packets and reduce the routing overhead. As number of selfish nodes increase, Routing overhead of overall network decrease drastically. Due to drastic decrement in routing overhead, overall network become efficient.

VI. CONCLUSIONS

We have simulated grey hole and forwarding node selfish behavior attacks on DSR protocol. The simulation of these protocols has been carried out using NS-2.34. We analyze both attacks in terms of network metrics like throughput, routing overhead and end to end delay.

The performance of routing protocols in MANET depends heavily on different kind of attacks. The results of simulation show that this attack has high effect on DSR protocol. In malicious attack case, if the number of attacker increases, the throughput is low, because grey hole attack is actually dropping data packets rather than routing packets.

Secondly, with our simulation study we find that in mobile ad hoc networks where route breakages are frequent, routing control packets consumes significant fraction of node energy and bandwidth. selfish behavior by certain number of nodes reduce the overall routing overhead in network which in turn result in resource saving for both, well behaving nodes and selfish nodes.

VII. REFERENCES

1. Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proceedings of Mobicom 2000, Boston, August 2000.
2. Toshihiro Suzuki, Motonari Kobayashi, Ashiq Khan, and Masanori Morita, "Proactive Cooperation Mechanism based on Cooperation Records for Mobile Ad hoc Networks", IEICE Transactions on Communication, Istanbul, June 2006; Volume E90.
3. David B.,Johnson David A.,Maltz Josh Broch "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", Ad Hoc networking, vol 5, pp 139-172,2001.
4. Levente Buttyan and Jean-Pierre Hubaux,"Enforcing Service Availability in Mobile Ad-Hoc WANs", 1st IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC 2000), Boston, MA, USA, 11 August 2000.
5. Mandalas, K.; Flitzanis, D.; Marias, G.F.; Georgiadis, P.; "A survey of several cooperation enforcement schemes for MANETs" , Signal Processing and Information Technology, 2005. Proceedings of the Fifth IEEE International Symposium on 21-21 Dec. 2005. Athens. pp. 466 – 471
6. Abdelaziz Babakhouya, Yacine Challal, Abdelmadjid Bouabdallah,"A Simulation Analysis of Routing Misbehavior in Mobile Ad Hoc Networks". 2008 IEEE, DOI 10.1109/NGMAST.2008.56.
7. Lei Guang and Chadi Assi, "Mitigating Smart Selfish MAC Layer Misbehavior in Ad Hoc Networks,"wimob, pp.116-123, 2006 IEEE International Conference on Wireless and Mobile Computing, Networking and Communication, 2006.
8. Tarag Fahad, Djamel Djenouri, Robert Askwith "On Detecting Packets Droppers in MANET: A Novel Low Cost Approach " in IAS'07 Proceedings of Third International Symposium on Information Assurance and Security.pp.56-64.2007.
9. Djamel Djenouri , Nadjib Badache. Two Hops ack: "New Approach for Selfish Nodes Detection in Mobile Ad hoc Networks". Technical report LSI-TRO704, University of Science and Technology houari boumediene, Algeria, April 2003.
10. Wei Yu and K. J. Ray Liu "Secure Cooperation in Autonomous Mobile Ad-Hoc Networks Under Noise and Imperfect Monitoring: A Game-Theoretic Approach ",IEEE transactions on information forensics and security, vol. 3, no. 2, june 2008.
11. Hyun Jin Kim and Jon M. Peha "Detecting Selfish Behavior in a Cooperative Commons",in Proceedings of IEEE DySPAN,pp. 1-12,2008.
12. A. A. C´ardenas, S. Radosavac, and J. S. Baras, "Detection and prevention of MAC layer misbehavior in ad hoc networks," in Proceedings of the 2nd ACM Workshop on

Security of ad hoc and Sensor Networks, SASN, Washington, DC, USA. ACM, 2004, pp. 17–22.

13. Wei Yu, K. J. R. Liu,Attack-resistant cooperation stimulation in autonomous ad hoc networks,Selected Areas in Communications, IEEE Journal on, Vol. 23, No. 12. (05 December 2005), pp. 2260-2271.
14. P. Michiardi and R. Molva, “CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks”, In Proc. 6th IFIP Commun. and Multimedia Security Conf., Sept. ’02.
15. S. Bansal and M. Baker. "Observation-Based Cooperation Enforcement in Ad-hoc Networks", Techical Report, Stanford University, ’03.
16. Lucent Technologies. “WaveLan IEEE 802.11 PC Card User’s Guide”. February, 1999.
17. L. M. Feeney & M. Nilsson `Investigating the Energy Consumption of a Wireless Network Intrface in an Ad Hoc Networking Environment'. IEEE INFOCOM-2001.
18. Jungkeun Yoon, Mingyan Liu, Brian Noble “Random Waypoint Considered Harmful'. IEEE INFOCOM-2003.
19. Andrej KOS, Janez BASTER, "Poisson Packet Generation based on Empirical Data", systmics,cybernetics and informatics, volume-1, number-5,2006.
20. Network Simulator Documentation at http://www.isi.edu/nsnam/ns/
21. Mobility Trace analyzer tools at http://nile.cise.u.edu/important/software.htm