Mr, Parth Wadhwa, Prof. Kajal S. Patel / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 2,Mar-Apr 2012, pp.1440-1442

Analysis of DoS Attack in DSR protocol

Mr, Parth Wadhwa
Information Technology Department,
SSIT college,
Bhavnagar, India

Prof. Kajal S. Patel
Computer Engineering Department,
L.D. College of Engineering,
Ahmedabad, India

Abstract— A wireless local area network (WLAN) links two or more devices using some wireless distribution method, and usually providing a connection through an access point to the wider internet. This gives users the mobility to move around within a local coverage area and still be connected to the network. Ad hoc networks are type of wireless LAN comprised of a group of workstations or other wireless devices which communicate directly with each other to exchange information. Mobile ad-hoc network (MANET) is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network. Nodes in mobile ad-hoc network are free to move and organize themselves in an arbitrary fashion. The path between each pair of the users may have multiple links and the radio between them can be heterogeneous. This allows an association of various links to be a part of the same network. Routing in ad hoc networks is nontrivial due to highly dynamic environment. In recent years several routing protocols targeted at mobile ad hoc networks which are DSDV, AODV, TORA, and DSR [1 2 5 6]. This paper does the comprehensive analysis of routing traffic generated using DSR routing and effect of Denial of Service attack in DSR [3 4]. Network has 4 fixed nodes in routing scenario. All nodes in the network are configured to manage UDP traffic. The result shows the amount of routing traffic generated.

Keywords-Ad hoc network, DSR,UDP, Service Attack, Denial of Service

I. INTRODUCTION

An ad hoc network is a collection of nodes forming a temporary network with out the aid of any additional infrastructure and no centralized control. The nodes in an ad hoc network can be a laptop, PDA, or any other device capable of transmitting and receiving information. Nodes act both as an end system (transmitting and receiving data) and as a router (allowing traffic to pass through) resulting in multi hop routing. [1] Network is temporary as nodes are generally mobile and may go out of range of other nodes in the network.

Routing in an adhoc network is nontrivial as they posses few characteristics [2] which make them different from wired networks. They are as follows:

- High probability of errors due to various transmission impairments
- Low Transmission range to conserve energy
- Frequent link breakages due to mobility
- Sleep period of operation of nodes and unidirectional links
- Unfavourable environmental conditions by virtue of applications of ad hoc networks
- Looping problem due to mobility
- No proper Addressing scheme

II. ABOUT DSR PTOTOCOL

A. DSR

Dynamic Source Routing (DSR) [3] is a reactive protocol i.e. it doesn't use periodic advertisements. It computes the routes when necessary and then maintains them. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which the packet has to pass; the sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host.

There are two significant stages in working of DSR: Route Discovery and Route Maintenance. A host initiating a route discovery broadcasts a *route request* packet which may be received by those hosts within wireless transmission range of it. The route request packet identifies the host, referred to as the *target* of the route discovery, for which the route is requested. If the route discovery is successful the initiating host receives a *route reply* packet listing a sequence of network hops through which it may reach the target. In addition to the address of the original initiator of the request and the target of the request, each route request packet contains a *route record*, in which is accumulated a record of the sequence of hops taken by the route request packet as it is propagated through the network during this route discovery.

While a host is using any source route, it monitors the continued correct operation of that route. This monitoring of the correct operation of a route in use is called *route maintenanc*e. When route maintenance detects a problem with a route in use, route discovery may be used again to discover a new, correct route to the destination.

To optimize route discovery process, DSR uses cache memory efficiently. Suppose a host receives a route request packet for

which it is not the target and is not already listed in the route record in the packet, and for which the pair (initiator address, request id) is not found in its list of recently seen requests; if the host has a route cache entry for the target of the request, it may append this cached route to the accumulated route record in the packet, and may return this route in a route reply packet to the initiator without propagating (re-broadcasting) the route request. The delay for route discovery and the total number of packets transmitted can be reduced by allowing data to be piggybacked on route request packets.

DSR uses no periodic routing advertisement messages, thereby reducing network bandwidth overhead, particularly during periods when little or no significant host movement is taking place. DSR has a unique advantage by virtue of source routing. As the route is part of the packet itself, routing loops, either short-lived or long-lived, cannot be formed as they can be immediately detected and eliminated [5].

III. DSR IN GLOMOSIM

In Glomosim 2.03 [7] we have basic MANET network model, you must configure the routing protocols on both the nodes and the routers in the network. All available MANET routing protocols provide loop-free, shortest path routing.

Available routing protocols in GLOMOSIM are:

- Dynamic Source Routing (DSR)
- Ad Hoc On Demand Distance Vector (AODV)
- WRP
- BELLMANFORD
- LAR1
- FISHEYE
- ZRP
- STATIC

DSR [3] is implemented at the IP layer. In GLOMOSIM, PROMISCUOUS-MODE defaults to YES and is necessary if nodes want to overhear packets destined to the neighboring node. Currently this option needs to be set to YES only for DSR is selected as routing protocol. Setting it to "NO" may save a trivial amount of time for other protocols.

IV. DENIAL OF SERVICE ATTACK

Many types of processes are used by the attacker to violate the security or make the system compromise with the security, which is known as Service Attacks [4], which is further dived into Active and Passive Attacks. Thus, to interrupt the service to be done, attacker use to send continuous message again that causes traffic in the path of transmission. This is known as denial of service attack, which is further categorized into SMARF Attack.

V. SIMULATION ENVIRONMENT

We use MANET model in GLOMOSIM [7] to simulate DSR network. The enterprise network with five WLAN nodes is deployed over a square geographical area with terrain dimension 1000m * 1000m. All the nodes in the network are configured to work under ad hoc mode. Among the 4 nodes, all 4 nodes are fixed ad hoc nodes having two source nodes and one destination node as shown in figure 1.

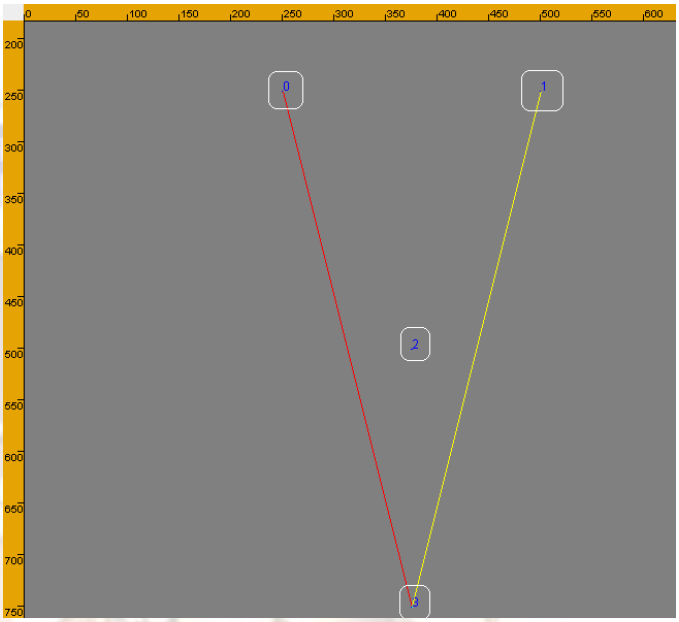

Figure 1. Simulation environment in GloMoSim

In UDP traffic the two originating nodes separately sends request and the neighboring or intermediate nodes send reply to the originating node to transmit data to the destination using the cached route updated in routing table.

UDP traffic is generated by configuring the app.conf file by adjusting constant bit rate (CBR) values.

CBR simulates a constant bit rate generator. In order to use CBR, the following attributes are needed:

- **Source** is the client node.
- **Destination** is the server node.
- **Items to send** is how many application layer items to send.
- **Item size** is size of each application layer item.
- **Interval** is the inter-departure time between the application layer items.
- **Start time** is when to start CBR during the simulation.
- **End time** is when to terminate CBR during the simulation.

If I**tems to send** is set to 0, CBR will run until the specified **End time** or until the end of the simulation, which ever comes first. If **End time** is set to 0, CBR will run until all **Items to send** is transmitted or until the end of simulation, which ever comes first. If **Items to send** and **End time** are both greater than 0, CBR will run until either **Items to send** is

done, **End time** is reached, or the simulation ends, which ever comes first.

VI. SIMULATION RESULTS

Simulation was run for 500 seconds for the scenario and the following results have been obtained to analyze the DSR routing traffic and Network load, when using customized file transfer based on UDP traffic.

Source node has initiated the route discovery process to send the request packet to the destination for downloading the files.

Table 1 shows the comparison of routing traffic sent in DSR network. This comparison is shown between two different cases as follows:

- Normal Situation
- Implementing DoS Attack

Attributes/Title	Normal Situation in DSR				Implementing DoS Attack			
	Nodes				Nodes			
	0	**1**	**2**	**3**	**0**	**1**	**2**	**3**
Packets Sent	75	75	0	0	75	75	0	0
Packets Received	0	0	0	150	0	0	0	0
Request Sent	2	1	1	0	70	70	0	0
Routes Selected	1	0	0	0	0	0	0	0
Hop Counts	2	0	0	0	0	0	0	0
Data Sent	75	75	150	0	0	0	0	0
Data Originated	75	75	0	0	0	0	0	0
Data Received	0	0	0	150	0	0	0	0
Packet Sent to MAC	76	77	152	1	70	70	0	0
Packets routed for another node	0	0	150	0	0	0	0	0
Total of TTL's of Delivered pac.	0	0	0	9300	0	0	0	0
Packets Dropped	0	0	0	0	75	75	0	0
Throughput	4151351351351				4151351			

Table. 1 Comparison of DSR in Normal Situation and after Implementing Attack

In Normal Situation, DSR broadcasts request from originating to the neighboring nodes to reach the destination. It selects the route through cached route path and sends the data to the intermediate nodes till it reach to the destination. Two originating nodes send data to destination at different time intervals. Thus, all the data is transmitted to destination successfully.

After implementation of DoS Attack in DSR, two originating nodes start sending data to the same destination at the same time interval till the end of simulation and thus create traffic. This traffic all packets are dropped causing the interrupt in service.

Throughput i.e., bits per second, is varied according to interval set for transmission and the way of transmission of packets.

VII. CONCLUSION

Following conclusion is made based on the analysis of simulation results. In general, the behavior of routing traffic is simulated and DSR network performance is analyzed using normal transmission of packets and after implementing smarf attack with no mobility environment.

After implementing denial of service attack,

- Thoughput is reduced.
- Routing Traffic is increased.
- Packets are dropped.
- Because of routing traffic, path loss occurs.

In future we can do the same analysis by adding more mobile nodes. We can also do analysis with some other type of Traffic after modifying DSR protocol.

REFERENCES

[1] J. Macker and S. Corson, Mobile Ad hoc Networks (MANET), http://www.ietf.org/charters/manet-charter.html, IETF Working Group Charter, 1997.

[2] S. R. Das, C. Perkins, and E. Royer, Performance comparison of Two On-demand Routing Protocols for Ad Hoc Networks, Proc. of IEEE INFOCOM 2000, March 2000.

[3] Mamoun Hussein Mamoun, A Secure DSR Routing Protocol in MANET, Jounal of Convergence Information Technology, March 2009.

[4] S. Bellovin, "Distributed Denial of Service Attacks", http://www.research.att.com/~smb/talks, Feb. 2000

[5] Academic Open Internet Journal ISSN 1311-4360 PERFORMANCE ANALYSIS OF ADHOC NETWORK ROUTING PROTOCOLS BY P. Chenna Reddy Dr. P. Chandrasekhar Reddy

[6] Piyush Gupta and P.R.Kumar,"The Capacity of Wireless Network",IEEE Transaction of Information Theory, March 2000

[7] A.Kathirvel, "Introduction to Glomosim" , Sep.2011