Simulating Broken Link Fraud in DSDV

H. Meena Sharma Rajbir Kaur M. S. Gaur
Department of Computer Engineering,
Malaviya National Institute of Technology,
Jaipur, Rajasthan, India- 302 017

ABSTRACT

A mobile ad hoc network (MANET) is a collection of mobile nodes forming an instant network with dynamic topology. Each mobile node acts as both router and host simultaneously. Routing protocols address the primary challenge of equipping each device to properly maintain information required to route traffic. Destination Sequence Distance Vector (DSDV) is one of the network layers routing protocol. Security is not addressed in DSDV making it vulnerable to various attacks. In this paper we discuss Byzantine and Broken Link Fraud in DSDV. We simulate Broken Link Fraud in ns-3 and show the effect of the attack on Packet Delivery Ratio (PDR). We show that PDR drops after the onset of the attack.

Key Words

MANETs, Byzantine attack, Broken Link Fraud, Denial of Services (DoS).

1. INTRODUCTION

A MANET [3] consists of mobile platforms referred to as “nodes”. Nodes are free to move about arbitrarily. MANET application areas include military or police exercise, disaster relief operations, mine site operations, robot data acquisitions. It is also used in inter vehicular communication where wired communication cannot be used due to high mobility. MANET nodes are equipped with wireless transmitters and receivers using antenna. At a given point in time, depending on the nodes’ positions, their transmitter and receiver coverage patterns, transmission power levels and co-channels interference levels, a wireless connectivity in the form of a random, multi-hop graph or “ad hoc” network exists between nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters.

In MANETs, routing protocol is deployed for the purpose of communication between mobile nodes. Routing protocol can be broadly classified as being reactive or proactive. In reactive protocol, routes are established when required e.g. AODV, DSR etc. Proactive protocol necessitates the maintenance of routing information all the time e.g. DSDV, OLSR etc. Proactive protocols are much faster and require more memory for delivery of information and storing routing information respectively. Reactive protocol takes more time for information delivery and memory requirement of reactive protocol is less compared to proactive protocol.

Destination Sequence Distance Vector (DSDV) [4] is a proactive protocol based on Bellman Ford algorithm [5]. DSDV is adapted from the conventional Routing Information Protocol (RIP) [6] to ad hoc networks routing. It adds a new attribute, sequence number to each route table entry of the conventional RIP. Using the newly added sequence number, the mobile nodes can distinguish stale route information. This prevents formation of routing loops.

Lack of inherent security mechanism make routing protocol vulnerable to attacks. In this paper we discuss two attacks on DSDV- Byzantine and Broken Link Fraud. In this attack the malicious node disrupts the appropriate working of the network affecting accurate packet delivery.

The rest of the paper is organized as follows. Section II introduces DSDV protocol, Section III discusses attack model in DSDV. In this section we discuss Byzantine attack and Broken Link Fraud. Section IV present related work. Section V discusses the simulation and results. In Section VI we describe our conclusions and future work. (In our paper the term misbehaving nodes, attacker nodes and malicious node mean the same).

2. DSDV PROTOCOL

Packets are transmitted between nodes in the network by using routing tables stored at each node. Routing tables at each node lists all available destinations in the network as well as the hop count to each. Each route table entry is tagged with a sequence number originated by the destination. To maintain the consistency of the routing tables in a dynamic varying topology each node transmits routing updates periodically (periodic updates). Routing updates are also broadcast immediately whenever significant new information is available (triggered updates).

In DSDV each route entry of the routing table contains the following information-

- Destination Node Address (*Dest*)
- Next Hop Address (*Next Hop*)
- Number of Hops to the destination (*Hop Count*)
- Time at which the entry was made (*Install Time*)
- Destination Originated Sequence Number (*Seq Num*)

All the nodes inter-operating to create data paths between themselves, broadcast the necessary data periodically. The data broadcast by each mobile node contains its new sequence number along with the following information for each new route:

- Dest
- Hop Count
- Seq Num

An even sequence number indicates a valid route while an odd one indicates a broken link.

A node updates its routing table based on the information received. Routes are selected according to the following criteria

- Route with higher sequence number is always preferred.
- For routes with same sequence number, the one with least hop count is selected.
- Routes with a sequence number less than the one already in the table is discarded as it is considered as a stale route

- Route received with odd sequence number is termed as a broken link.

In order to reduce the information carried in a routing packet, two types of packets are defined

- Full Dumps: contains all the available routing information
- Incremental Dumps: Carry information changed since last full dump

Figure 1 shows an example of mobile ad hoc network consisting of seven nodes. Let N1 be the source node and N7 be the destination node. There are two routes from N1 to N7

- Route 1: N1->N2->N6->N7
- Route 2: N1->N3->N4->N5->N7

If sequence number of Route 2 is greater than the sequence number of the Route1, Route 2 is preferred even though it has a higher hop count. If sequence number of Route 1 is equal to the sequence number of Route 2, Route 1 is preferred as it has lower hop count.

3. ATTACK MODEL IN DSDV

Routing in DSDV is based on multi-hop forwarding. Intermediate node forwards data packets from source to destination. The nodes trust each other. Information received from neighboring nodes is always considered to be valid. Misbehaving node exploit this to fabricate the data when it is one of the intermediate node. Misbehavior can be in the form of dropping the packets, injecting new packets or even changing the packets contents.

In this section we describe two attack models against DSDV.

- Byzantine Attack
- Broken Link Fraud

Byzantine Attack: Byzantine attack [9] can be defined as attack against routing protocol in which misbehaving nodes use effective strategies to drop, fabricate, modify or misroute the packages in an attempt to disrupt routing services. In DSDV the misbehaving node is able to disrupt routing services by first including itself in the path to destination. This can be accomplished in two ways:

- Advertise a path to destination with lower hop count
- Advertise a path to destination with higher sequence number

Once the misbehaving node is included as an intermediate node in the route to destination, it is entrusted with the responsibility to forward packet. The malicious node may in turn disrupt routing by dropping or modifying packets.

Broken Link Fraud: Broken Link Fraud [10] is a denial of service attack wherein a misbehaving node targets an honest node by propagating an infinite distance to it. The result is that the target node never features in the path to the destination or as destination itself.

Consider the topology in figure 1. Let N1 be the source, N7 the sink and N4 the misbehaving node. N4 advertises a broken link to N7. The other nodes are forced into believing that N7 is unreachable.

Table I shows fake table advertised by N4 indicating a broken link to N7.

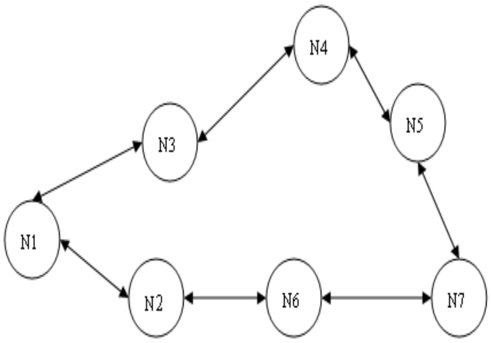

Figure 1. An Ad hoc network

TABLE I Fake Routing information Propagated by N4

Destinatio n	Next Hop	Sequence Number	Hop Count
N1	N3	4	2
N2	N3	4	3
N3	N3	4	1
N4	N4	8	0
N5	N5	6	1
N6	N5	6	3
N7	N5	9	∞

Broken Link Fraud is launched in two phases.

Phase 1: Attacker node becomes the intermediate node in the route from source to destination.

The misbehaving node includes itself in the legitimate path between the source and destination. To achieve this it employs the following mechanism:

- advertises itself to be the node which is nearest to the destination through smaller hop count
- advertises itself to be the freshest route through higher sequence number
- Fake routing information is broadcast in the form of triggered or incremental updates. DSDV always prefers route with a highest sequence number. Attacker is able to include in the route to a particular destination.

Phase 2: Attacker propagates destination as broken link

Misbehaving node propagate infinite distance for the destination with an odd sequence number. Nodes in the network update their routing table with this information.

4. RELATED WORK

Wang et al [7] have studied the security properties of DSDV by simulating false distance vector and false destination sequence attacks.

In [8] Kumar discusses following threats to distance vector routing protocols.

- Intruder modifies information in routing update
- packets to disrupt communication
- Intruder replays old routing updates or destroys
- routing message update at random
- Intruder reroutes traffic to a particular location taking
- the role of source or destination

5. SIMULATIONS AND RESULTS

In this section we describe the simulation environment used to model Broken Link Fraud on DSDV. Results are also reported and analyzed.

5.1. Simulation Setup

We use ns-3 [1] simulator to simulate our attack model. Here we have considered a network size of 16 nodes, placed

in a square area of 1000 m * 1000 m. Each node is moving according to random way point mobility model with a speed of 10 m/sec. We use UDP traffic type. The source sends packet at the rate of 1 packet/sec to the destination. Data packets are sent from the 5th second onwards after the start of simulation. Here we assume that attacker exhibit malicious behavior from the start of simulation. We vary the duration of the simulation from 60-200 seconds in the steps of 10 seconds. Table II lists simulation parameters used.

5.2. Implementation of Broken Link Fraud

DSDV implemented in ns-3 describes a route as broken rink if the sequence number of that route is odd. A node updates the broken link information about a destination if and only if it comes from its next hop neighbor; else the update received is discarded. In ns-3, each node maintains two types of table:

TABLE II Simulation Parameters

Simulator	ns-3.9
Number of nodes	16
Mobility Model	Random way Point
Traffic Type	UDP
Packet Size	1000 Bytes
Data Rate	8Kbps
Node Speed	10m/sec
Area	1000 m *1000 m
Simulation Durations	60-200 seconds

- Main table: Maintains routing information related to the node.
- Advertised table: The table that is broadcast in the network. Hop count of all destinations is incremented by 1 before broadcast.

We implemented the attack as follows:

- The attacker (say, a1) broadcasts route to destination (say, d1) with a higher sequence number from the start of simulation in triggered updates.
- Nodes in the network prefer routes with higher sequence number and update their routing tables with fresh information. Next hop neighbor in routing entry for d1 is set to a1. Sequence number is also updated to that broadcast by a1.
- a1 broadcasts d1 as broken link in periodic updates.

When a node (say, n1) receives an update specifying d1 as broken link, n1 verifies the sender of the update. If the update comes from n1s next hop neighbor, then

- Route entry for d1 is deleted from n1s main routing table
- Sequence number of the route entry for d1 in n1s advertised table is updated. The sequence number is set to the odd sequence number received in the update.
- Triggered update announcing d1 as broken link is broadcast to the network

This fake information is disseminated through out the network. a1 has already advertised itself as next hop to other nodes in the network. Nodes update their routing table with fake fresh information. The result is that the target node d1 becomes unreachable.

When an attacker attacks a proactive protocol, it has to routinely update the fake route to keep it alive [7]. To maintain the impact of Broken Link Fraud in ns-3, we modify the DSDV code such that the attacker broadcast broken link i.e. an odd sequence number to the target node in the periodic updates. To become the intermediate node in the path between source and sink, attacker node carries out Byzantine attack. This is done by manipulating the information in triggered updates. Thus attacker has to frequently broadcast fake route through itself to become intermediate node in the route between source and sink and then broadcast broken link to the target node.

5.3. Performance Evaluation

The performance metric is defined as follows.

Packet Delivery Ratio (PDR): The ratio of the total numbers of packets successfully delivered to the destination to the total number of packets sent out by the source node.

5.4. Simulation Results

It is observed from the graph in figure 2 that PDR drops drastically when the network is under attack. Packets intended for sink (target) cannot be delivered as it has been broadcast as broken link. Attacker causes disruptions in the normal delivery of packets to the sink thereby exhibiting a Denial Of Service attack.

6. CONCLUSION AND FUTURE WORKS

In this paper we have discussed that lack of security mechanisms in DSDV makes it prone to attack. We have discussed Byzantine attack and Broken Link Fraud in DSDV. We show by simulation that Broken Link Fraud is a DoS attack that creates a great dip in PDR. In the future we aim to develop a methodology for mitigating the impact of Broken Link Fraud.

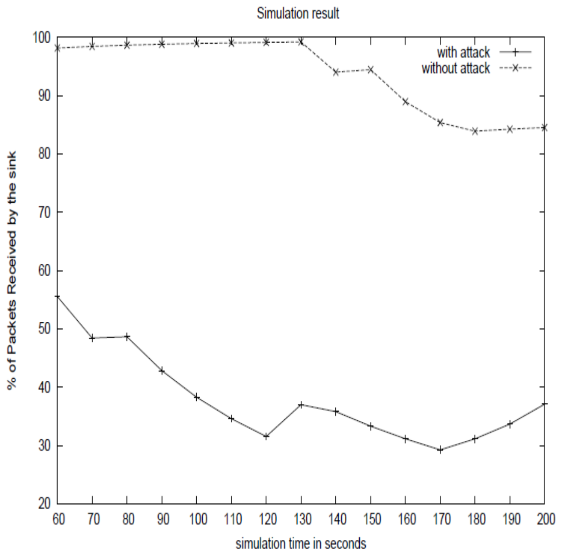

Figure-2 : Comparison of PDR during attack and normal scenario against different simulation duration

7. REFERENCES

[1] Network simulator 3. http://www.nsnam.org.

[2] MANETs http://en.wikipedia.org/wiki/Mobile_ad_hoc_network

[3] Mobile Ad hoc Networking (MANET): Routing protocol Performance Issues and Evaluation Considerations. http://www.ietf.org/rfc/rfc2501.txt

[4] Charles E.Perkins and Pravin Bhagwat. "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers" SIGCOMM Comput. Commun. Rev. , pp 234-244, 1994

[5] Richard Bellman, "On a Routing Problem", Quarterly of Applied Mathematics, pp. 87–90, 1958.

[6] C.Hedrick. "Routing Information Protocol". RFC 1058. Technical report, IETF, June 1988.

[7] Wang Weichao, Yi Lu, and B Bhargava. "On Security Study of Two Distance Vector Routing Protocols for Mobile Ad Hoc Networks". In proceedings of the first IEEE International Conference on Pervasive Computing and Communications, pp. 179-186, March 2003

[8] Brijesh Kumar. "Integration of Security in Network Routing Protocol" SIGSAC Rev. pp 18-25, 1993

[9] Baruch Awerbuch, Reza Curtmola, David Holmer, Cristina Nita Rotaru, and Herbert Rubens, " Mitigating Byzantine Attacks in AdHoc Wireless Networks". Technical report, Department of Computer Science, Johns Hopkins University, Tech, 2004.

[10] Rajbir Kaur, Manoj Singh Gaur, and Vijay Laxmi. "A Novel Attack Model Simulation in DSDV Routing". In Proceedings of the 4th IFIP International Conference on New Technologies, Mobility and Security[Communicated and Accepted], volume IEEE Xplore, February 2011.