Understanding Vulnerability of Adhoc Networks Under Malicious Node Attacks

Mozmin Ahmed[1]
North Eastern Regional Institute of Science and Technology, Itanagar,
Arunachal Pradesh, India 791109

Dr. Md. Anwar Hussain[2]
North Eastern Regional Institute of Science and Technology, Itanagar,
Arunachal Pradesh, India 791109

Abstract- As the importance of the mobile ad hoc network is growing and their usage is increasing in sensitive applications like military, disaster relief, Tsunami, the issues of security has become important. The routing in MANETs which is already complex due to multi hop nature of ad hoc network faces a lot of problems in terms of security.

In this paper we have simulated Ad hoc Network under various conditions and tabulated the throughput and packet drops of the nodes in the network under each condition. This enables us to understand the network vulnerability under the malicious node attack and the network behavior thereafter.

We made a study of malicious node attack under three different scenarios. 1. Increase group size along with increase in number of malicious nodes. 2. Increase group size keeping number of malicious nodes constant. 3. Keeping fixed group size and increase in number of malicious nodes. The malicious node would simply drop any packets it receives for onward transmission, thus making the network insecure. We observe unique attack patterns under different scenarios.

INTRODUCTION

Adhoc networks have no supporting infrastructure. Adhoc network are comprised of a dynamic set of co-operating peers, which share their wireless capabilities with other similar devices to enable communication with devices not in direct radio range of each other.

The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting multi hop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. The AODV routing protocol is designed for mobile ad hoc networks with populations of ten to thousands of mobile nodes. AODV can handle low, moderate and relatively high mobility rates, as well as variety of data and traffic levels.

Ad hoc networks are by nature very open to anyone. Their biggest advantage is also one of their biggest disadvantages: basically any one with proper hardware and knowledge of the network topology and protocols can connect to the network. This allows potential attackers to infiltrate the network and carry out attacks on its participants with purpose of stealing or altering information.

In an Ad hoc network malicious nodes may enter and leave the immediate radio

transmission range at random intervals or may collude with other malicious nodes to disrupt network activity and avoid detection. Malicious node may behave maliciously only intermittently further complicating their detection. The loss or capture of unattended sensors and personal computing devices may allow for a malicious node to obtain legitimate credentials and launch more serious attacks. A node that sends out false routing information could be a compromised node, or merely a node that has temporarily stale routing table due to volatile physical conditions.

Attacks can be targeted at the routing protocol in which the malicious node actively disrupts the functioning of the co-operative routing mechanisms. A secure routing protocol is intended to minimize or prevent the impact of possible attacks against nodes in a MANET.

In general the attacks can be classified as:

1. Routing Disruption Attacks : A malicious node intentionally drops control packets, misroutes data, or disseminates incorrect information about its neighbours and/or its pre discovered routing capabilities to particular destinations.

2. Resource Consumption Attacks : An attacker might try to consume network resources by initiating large number of route requests to bogus destinations and playing the "Gray hole attack" or "selective dropping" of packets, resulting in increased number of route requests from neighbor nodes.

3. Attacks on Data Traffic: A group of malicious nodes can collude in attacking the network causing far more damage than a single node.

Typical attacks are "Wormhole Attack", "Invisible Node Attack" and "Rushing Attack".

We restrict the non-malicious nodes in different quadrants in groups of a fixed number, and the members of the group are free to move or remain static only in that quadrant. The malicious nodes, however, are free to move through all the four quadrants and attack any node pair's communications. The simulation is carried out using Network Simulator NS 2.31 in Debian Linux 4 using AODV routing protocol.

IMPLEMENTING ATTACKS ON AODV ROUTING PROTOCOLS

In our work, we have simulated malicious node that drops all the packets which passes through it. We have created malicious nodes in AODV protocol by modifying the aodv.cc and aodv.h files.
In aodv.h file we add "bool malicious" in the program as follows. This variable is used to define whether the node is malicious or not.

```
/*
 * History management
 */

bool    malicious;

double PerHopTime(aodv_rt_entry *rt);


nsaddr_t        index;          // IP
Address of this node
u_int32_t       seqno;          //
Sequence Number
```

```
int          bid;                    //
Broadcast ID

aodv_rtable      rthead;        // routing
table
aodv_ncache      nbhead;        //
Neighbor Cache
aodv_bcache      bihead;        //
Broadcast ID Cache
```

In **aodv.cc** we add the line "malicious = false;". This line is added as initially nodes are not malicious and we need to add the line to define which node is malicious.

```
/*
  Constructor
*/

AODV::AODV(nsaddr_t id) :
Agent(PT_AODV),
        btimer(this), htimer(this),
ntimer(this),
         rtimer(this), lrtimer(this), rqueue()
{


 index = id;
 seqno = 2;
 bid = 1;
 malicious = false;
 LIST_INIT(&nbhead);
 LIST_INIT(&bihead);

 logtarget = 0;
 ifqueue = 0;
}
```

Now we need to add the line to catch the nodes which are malicious. We add the line "malicious = true"

```
int
AODV::command(int argc, const
char*const* argv) {
        if(strcmp(argv[1], "hacker") == 0)
{
        malicious = true;
        return TCL_OK;
        }
        if(argc == 2) {
          Tcl& tcl = Tcl::instance();

  if(strncasecmp(argv[1], "id", 2) == 0) {
    tcl.resultf("%d", index);
    return TCL_OK;
   }
if(strcmp(argv[1], "hacker") == 0) {
return TCL_OK;

}
```

Now we need to define what a malicious node should do. Here in this case we want that the malicious node should drop any packet that is received. We define this in Route Handling Functions.

```
/*
 Route Handling Functions
*/

void
AODV::rt_resolve(Packet *p) {
struct hdr_cmn *ch = HDR_CMN(p);
struct hdr_ip *ih = HDR_IP(p);
aodv_rt_entry *rt;

// if I am malicious node
if (malicious == true ) {
drop(p, DROP_RTR_ROUTE_LOOP);


/*
DROP_RTR_ROUTE_LOOP is added for
no reason.
*/
}
```

In our TCL file we define malicious node with following command.

$ns at 0.0 "[$node_(5) set ragent_] hacker" This command defines the node (5) to be malicious and drop all the packets.

After the modifications in the aodv.cc and aodv.h file we recompile and install the program using makefile.

SIMULATIONS, RESULTS AND ANALYSIS

In this section we describe the simulation scenarios under which the malicious nodes were introduced. We run the simulation varying the group size, number of malicious nodes, and extract the throughput and drop rate for each simulation from the trace files. The simulations were carried out under the following parameters. The same simulation is repeated for each scenario with two different node positions. This enables us for better understanding of the network with active malicious nodes.

Table 1 : AODV Scenario Parameters.

Traffic Pattern	FTP
Simulation Area	800 m by 640 m
Simulation Time	200 seconds
Total Nodes	20 ~ 100
No of Groups	4
Total Malicious Nodes	4~ 20
Total Senders	4
Total Receivers	16~96
Total Connections	16~96
The Data Packet Size	64 bytes
MAC Layer	IEEE 803.11
No. of Cases for One Scenario	5
Node Mobility	1~10 m/sec

The initial and final node positions are defined and Nodes move from their initial position to the final position in a straight line. In this simulation the non-malicious as well as the malicious nodes are free to move in any quadrant. The speed of all nodes is defined for uniform movement. We show below the three different scenarios under which the simulations were carried out. The results are tabulated and a few graphs are plotted below for better understanding of the simulation under malicious attack.

The average throughput is calculated using the Perl script file. All the packets transmitted from all the nodes is added and averaged out over the time of simulation. The results thereby obtained are tabulated and plotted.

Similarly the average packet drop is calculated using a different Perl script file. The total packets dropped in the simulation from all the nodes are added. The figure is averaged over the simulation period.

Scenario 1: We increase the group size and simultaneously increase the number of malicious nodes.

To understand the effect of the initial positions of the nodes, we carried out two simulations for two different starting (initial) positions of the nodes.

Table 2

Case No.	No. of groups	Group				Scenario			
		Total Members	No. of Senders	No. of receivers	No. of Malicious Nodes	Total Members	No. of Senders	No. of receivers	No. of Malicious Nodes
1	4	5	1	4	1	20	4	16	4
2	4	10	1	9	2	40	4	36	8
3	4	15	1	14	3	60	4	56	12
4	4	20	1	19	4	80	4	76	16
5	4	25	1	24	5	100	4	96	20

The throughput achieved during the above five simulations is shown in the Figure 1 and Figure 2, for the two different starting node positions, respectively.

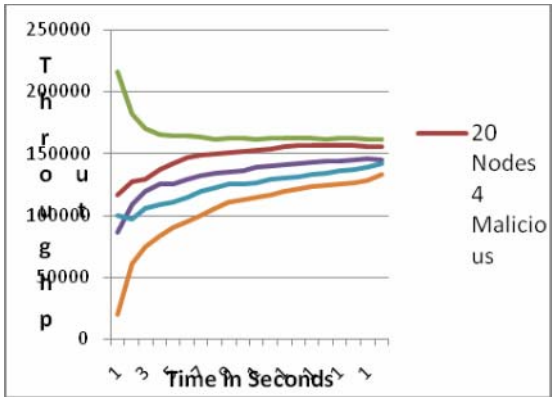


Figure 1 (Under first Initial node positions)

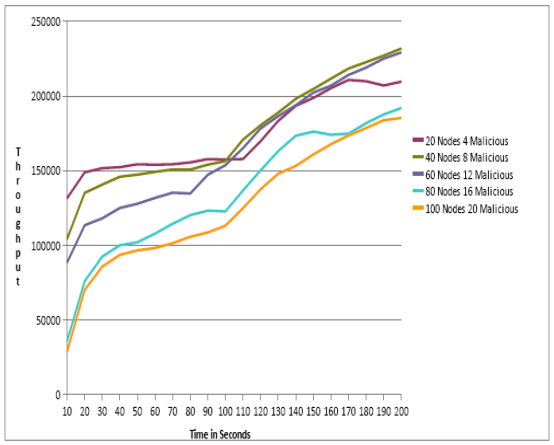


Figure 2 (Under new initial node positions)

The average drop for the five simulations is shown in Figure 3 and Figure 4 respectively.

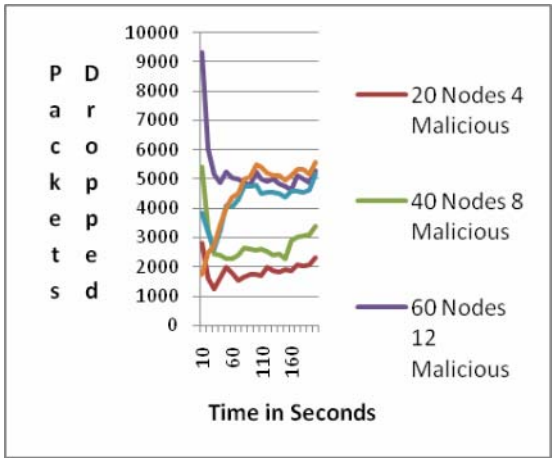


Figure 3 (Under First Initial node positions)

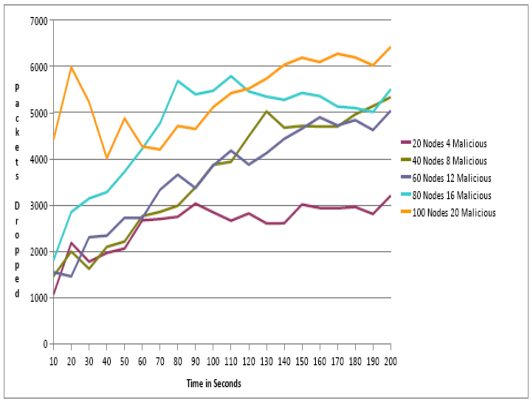


Figure 4 (Under new initial node positions)

Scenario 2 : We increase the group size and keep the number of malicious nodes constant.

Table : 3

Case No.	No. of groups	Group				Scenario			
		Total Members	No. of Senders	No. of receivers	No. of Malicious Nodes	Total Members	No. of Senders	No. of receivers	No. of Malicious Nodes
1	4	5	1	4	1	20	4	16	4
2	4	10	1	9	1	40	4	36	4
3	4	15	1	14	1	60	4	56	4
4	4	20	1	19	1	80	4	76	4
5	4	25	1	24	1	100	4	96	4

The throughput achieved from the above five simulations is shown in the Figure 5 and Figure 6 respectively.

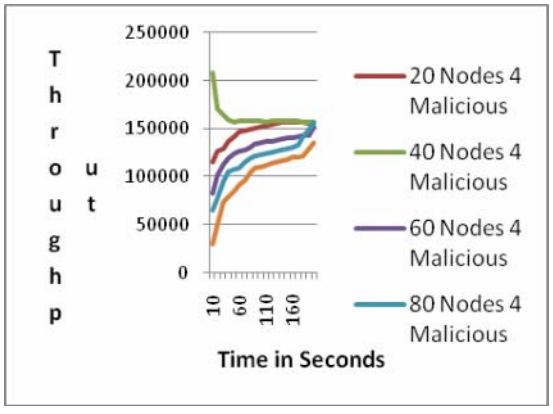


Figure 5 (Under First Initial node positions)

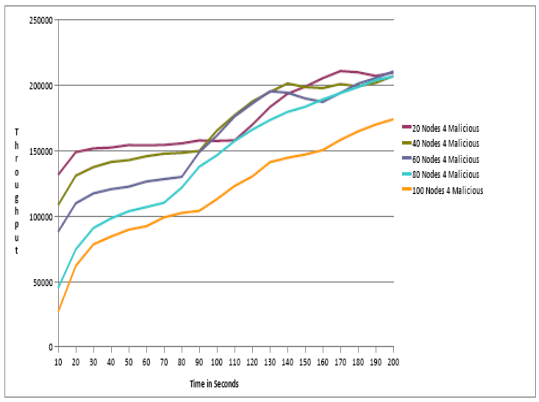


Figure 6 (Under new initial node positions)

The average drop for the five simulations is shown Figure 7 and Figure 8 respectively.

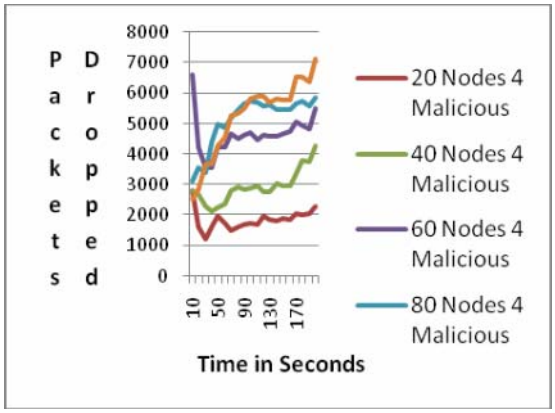


Figure 7 (Under First Initial node positions)

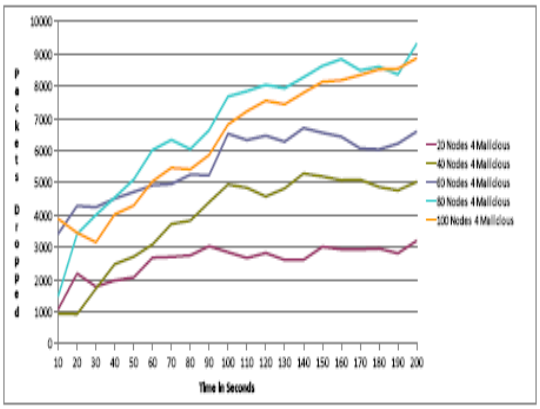


Figure 8 (Under new initial node positions)

Scenario 3 : We keep the group size fixed and increase the number of malicious nodes.

Table 4

Case No.	No. of groups	Group				Scenario			
		Total Members	No. of Senders	No. of receivers	No. of Malicious Nodes	Total Members	No. of Senders	No. of receivers	No. of Malicious Nodes
1	4	25	1	24	1	100	4	96	4
2	4	25	1	24	2	100	4	96	8
3	4	25	1	24	3	100	4	96	12
4	4	25	1	24	4	100	4	96	16
5	4	25	1	24	5	100	4	96	20

The throughput achieved from the above five simulations is shown in Figure 9 and Figure 10 respectively.

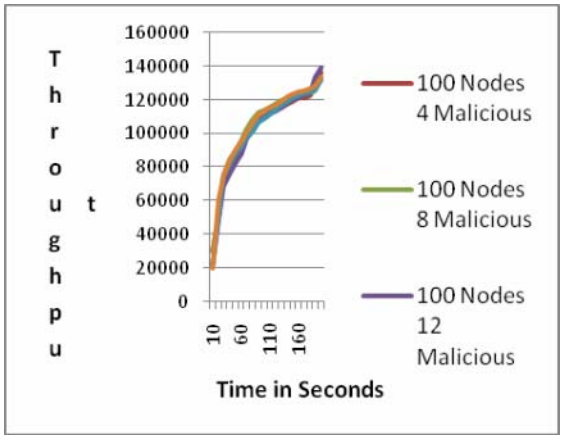


Figure 9 (Under First Initial node positions)

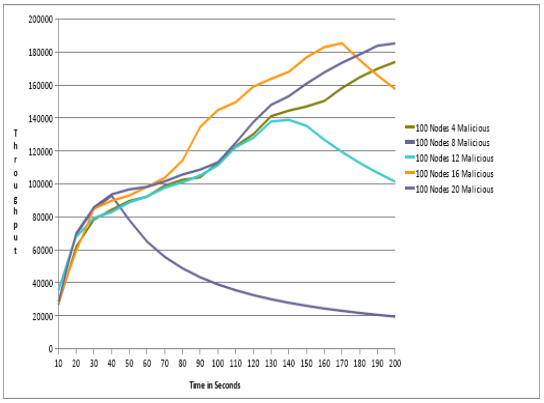


Figure 10 (Under new initial node positions)

The average drop for the five simulations is shown in Figure 11 and Figure 12 respectively.

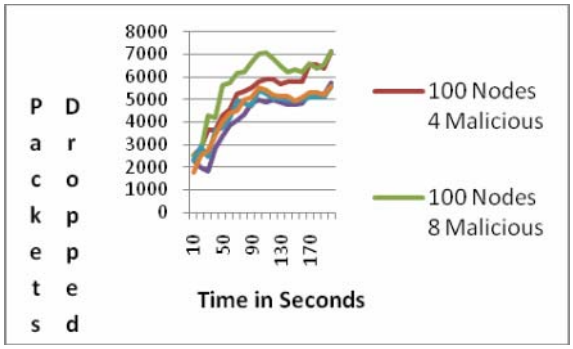


Figure 11 (Under First Initial node positions)

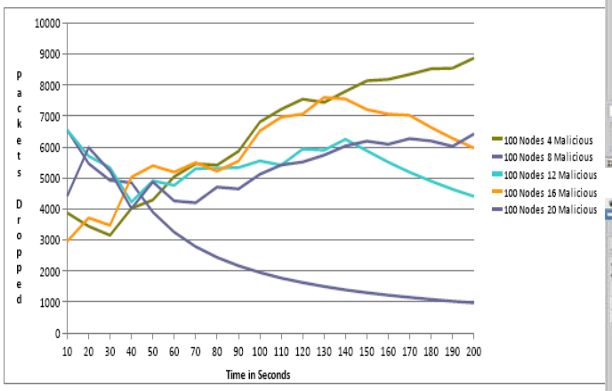
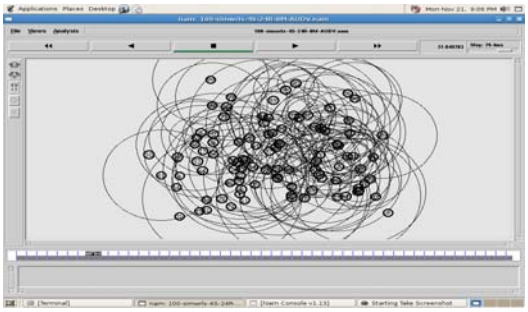


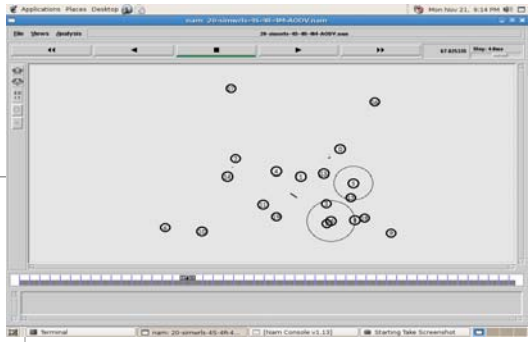
Figure 12 (Under new initial node positions)

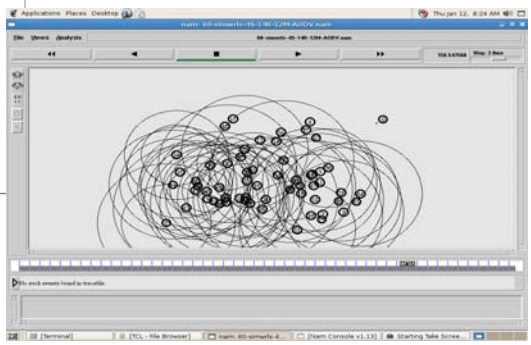
CONCLUSION

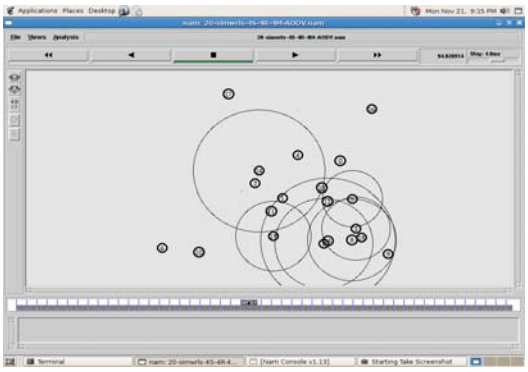
In this study, we have analyzed the different effect of the attacks of malicious nodes in Ad hoc networks under various conditions. From the tables and the graphs plotted through the simulations, we are able to identify the pattern the malicious attacks. Providing security in mobile adhoc networks (MANETS) is a prime concern due to the need of providing protected communication in a hostile environment. With the attack pattern under our study we should be able to implement an efficient algorithm for intrusion detection system which would use collaborative efforts of nodes in a neighborhood to detect a malicious node.

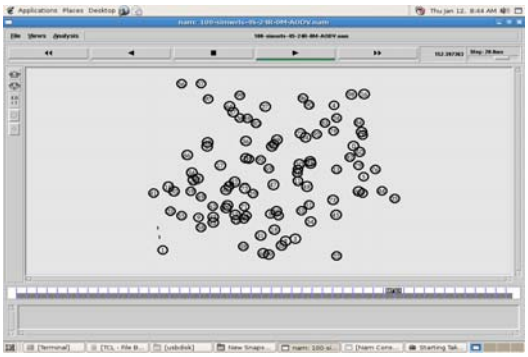
A few of the snap shots taken during the simulation are shown below.

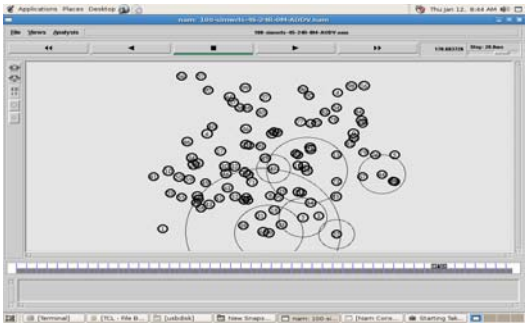












FUTURE WORK

The simulation may be extended with practical cases of random distribution of the nodes. The speed may be varied and the space of simulation can also be changed to study the network behaviour. We are working on a practical example by varying the speed equivalent to walking speed of a man compared to high speed moving vehicle. The random simulation may be repeated number of times and the results obtained thereby can be averaged and tabulated for more realistic network behavior results.

REFERENCES

[1]. Reza Curtmola and Cristina Nita-Rotaru " BSMR: Byzantine-Resilient Secure Multicast Routing in Multi-hop Wireless Networks" March 2007.

[2]. The *ns* Manual (formerly *ns* Notes and Documentation).

[3]. The Network Simulator, http://www.isi.edu/nsnam/ns

[4]. Charles E-Perkins And Elizabeth M_Royer Ad_hoc On_Demand Distance Vector Routing.

[5]. Kurose, Ross "How To Misuse Aodv: A Case Study Of Insider Attacks Against Ad- Hoc Routing Protocols".

[6]. Security in Mobile Ad Hoc Netwroks – Rudi Belloti, Frank Lyner, April 29, 2003.

[7]. A survey of Routing Attacks in Mobile Ad Hoc Networks – Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaka Nemoto, Nei Kato, and Abbas Jamalipour.

[8]. "Adding Malicious Node to AODV"- Elmurod A. Talipov.