IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 6, Ver. I (Nov – Dec. 2015), PP 55-63
www.iosrjournals.org

Impact of Malicious Nodes on Throughput, Packets Dropped and Average Latency in MANETs

Md. Razibuddin Ahmed[1,] Mozmin Ahmed[2]
McLeod Russel India Limited, Kolkata, West Bengal, India 700001
North Eastern Regional Institute of Science and Technology, Itanagar,
Arunachal Pradesh, India 791109

Abstract:- *Mobile Ad-hoc Network is a decentralized wireless network[1]. Here the mobile nodes make and break the links with the neighbouring nodes available in the radio range without actually being physically connected. These networks are temporary and keep on changing from time to time. MANET applications are getting importance in both civilian and military areas. MANETs can be applied in disaster communications and used as the backup network of traditional mobile communication networks as well. Network throughput, number of packets dropped and average latency are important parameters to evaluate the performance of wireless ad hoc network[3]. Generally, it is difficult to achieve high throughput and low packet drop with minimum delay[5]. In this paper, the objective is to achieve high throughput while keeping the packet drop and the average latency under certain acceptable limits[10]. We tried to study the signature pattern of these malicious nodes and made conclusions with the results obtained. The performance is evaluated with the following parameters: network throughput, number of packets dropped and the average latency. We used NS2 simulator and extracted data from the trace files[2]. Ad-hoc On Demand Distance Vector (AODV) routing protocol has been used in our experiments[4]. Similar to our previous work, the nodes are free to move or remain static in all the quadrants in the defined space[8].*

Keywords: *MANET, Malicious Node, AODV routing Protocol, Network Throughput, Packets Dropped, Average Latency, NS2.*

I. Introduction

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

Malicious node disrupts the network activity in ad hoc networks. 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 condition. A malicious attacker can readily become a router and disrupt network operations by its malicious activity like the black hole attack, gray hole attack, worm hole attack, sink hole attack etc[6]. We need to identify the malicious behavior of the system and isolate the misbehaving node as quickly as possible so that the communication through the network is not affected.

The performance and use of wireless technologies has increased tremendously, opening up avenues for application in the less explored areas. MANET is one important field of concern, in which the mobile nodes organize themselves in a network without the help of any predefined infrastructure. Securing MANETs is an important part of deploying and utilizing them since, MANET is used in critical applications where data and communication integrity is important. Existing solutions for wireless networks can be used to obtain a certain level of such security. Nevertheless, these solutions may always be sufficient, as ad hoc network have their own vulnerabilities which cannot be addressed by these solutions.

II. Implementing Aodv Routing Protocols

Simulation Environment:

We have created a simulation program with 20 nodes. These 20 nodes are divided into four groups with five members in each group. Out of the five nodes in a group, one node is the source node and the other four are the receiver nodes. In the beginning, the source node sends information to its group members lying within its radio range. The movement of the five nodes in each group is limited to its own designated area. The receiver nodes broadcast the message to its immediate neighbours within the range once it receives any information from the source node or any other forwarding node acting as a router. We implemented this scenario using AODV routing protocol and studied the performance of the network considering the parameters: network throughput, packets dropped and average latency. The scenario is shown below:

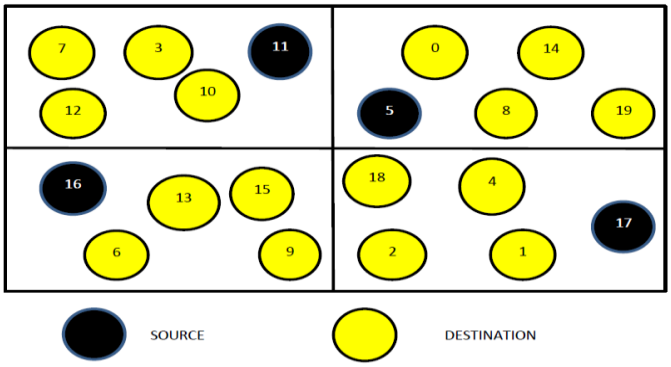

Figure 1: Network with four groups each having one source and four destination nodes.

We further increased the group size keeping two groups with one source and nine receiving nodes in each group. Two nodes in the scenario showing malicious behaviour in each group dropped all packets it received without any further communication. All the nodes could freely move around in the entire simulation area. This scenario was implemented using AODV routing protocol. Simulations were carried out to study the performance with respect to the network throughput, packets dropped and average latency. The scenario is shown below.

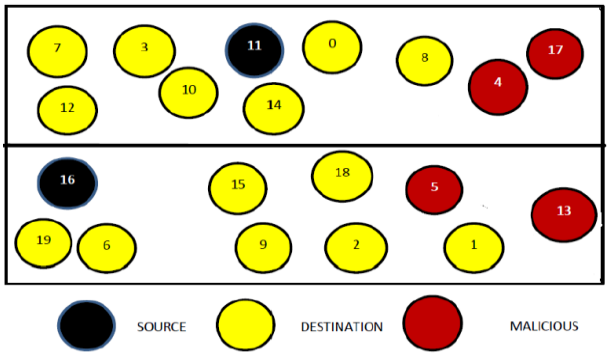

Figure 2: Network with two groups each with one source, nine destinations with two malicious nodes.

The scenario was extended with 100 nodes in the network divided into four groups[9]. Each group had one source and twenty-four receivers. Thus, the maximum group size in our simulations was of twenty-five members. Amongst the receiver nodes, a few nodes were programmed to show malicious behavior[7]. We study the performance of the network under various changing parameters by repeating the simulations for ten times under each case. Each simulation was run for 200 seconds. We plotted graphs from the average results of these ten simulations for the throughput, packet drop and delay. The main goal of our simulation was to model the behaviour of AODV protocol without malicious nodes and with malicious nodes. The simulation space was kept at 2000m X 800m. The mobility of the nodes varied from 1m/sec to 10m/sec.

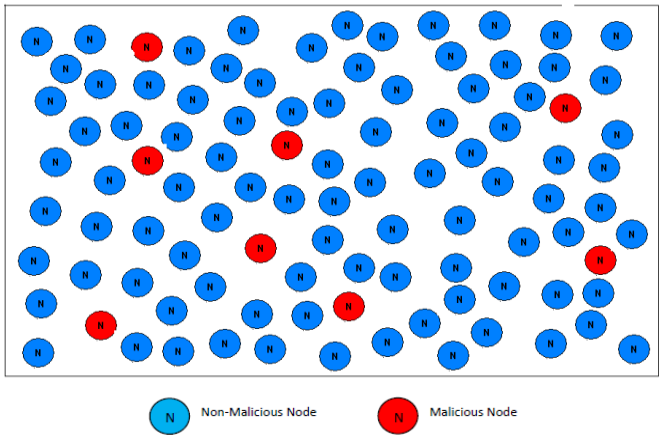

Figure 3: Distribution of Eight Malicious Nodes

System requirements and specifications

Processor	:	Intel(R) Core(TM) i3 CPU M 380 @ 2.53 GHz processor
RAM	:	3.00 GB
Hard Disk	:	80 GB
Input Device	:	Standard Keyboard and Mouse
Output Device	:	LCD Monitor

Software Requirement

Software	:	NS-2.35
Operating System:		Debian Linux 4

The number of malicious nodes in each group was increased from zero to ten nodes. The result of each simulation is extracted from the trace file. We have developed perl programs to extract data for the average latency, network throughput and packets dropped from the trace files.

III. Simulations, Results And Analysis

Table 1 : AODV Scenario Parameters.

TRAFFIC PATTERN	FTP
SIMULATION AREA	2000m X 800m
SIMULATION TIME	200 Seconds
TOTAL NODES	100 Nos.
NUMBER OF GROUPS	4 Nos.
TOTAL SENDERS	4 Nos.
TOTAL RECEIVERS	96 Nos.
TOTAL CONNECTIONS	96 Nos.
NUMBER OF MALICIOUS NODES	4 to 40 Nos
THE DATA PACKET SIZE	64 BYTES
MAC LAYER	IEEE 802.11
NUMBER OF CASES FOR ONE SCENARIO	11 Nos.
NODE MOBILITY	1m/sec to 10m/sec

The initial and the final node positions along with the speed of the nodes were pre-defined. Nodes moved from their initial position to the final position in a straight line.
During our experiment, we have observed that if any vital node was defined as malicious, the system tripped with a message and the program gets terminated. We thus had to repeat the simulation by changing the position of the malicious node after observing the nam plots. Some of the errors noted are given below;

root@Mozmin-PC:/home/mozmin/NS/ns-allinone-2.35/TCL Files 9# num_nodes is set 100
num_nodes is set 96
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5, distCST_ = 550.0

SORTING LISTS ...DONE!
MAC_802_11: accessing MAC cache_ array out of range (src 96, dst 66, size 96)!
MAC_802_11: accessing MAC cache_ array out of range (src 97, dst 63, size 96)!
MAC_802_11: accessing MAC cache_ array out of range (src 98, dst 68, size 96)!
MAC_802_11: accessing MAC cache_ array out of range (src 97, dst 63, size 96)!
MAC_802_11: accessing MAC cache_ array out of range (src 97, dst 80, size 96)!
MAC_802_11: accessing MAC cache_ array out of range (src 97, dst 80, size 96)!
MAC_802_11: accessing MAC cache_ array out of range (src 99, dst 27, size 96)!
MAC_802_11: accessing MAC cache_ array out of range (src 97, dst 80, size 96)!
MAC_802_11: accessing MAC cache_ array out of range (src 97, dst 63, size 96)!
MAC_802_11: accessing MAC cache_ array out of range (src 97, dst 63, size 96)!
[suppressing additional MAC cache_ warnings]

```
root@Mozmin-PC:/home/mozmin/NS/ns-allinone-2.35/TCL Files 9# num_nodes is set 96
num_nodes is set 100
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
root@Mozmin-PC:/home/mozmin/NS/ns-allinone-2.35/TCL Files 9# check_pktTx:Invalid MAC Control
subtype
[1]+  Exit 1                  ns 100nodes-4S-24R-4M-AODV-TCP-ran-20008001.tcl

root@Mozmin-PC:/home/mozmin/NS/ns-allinone-2.35/TCL Files 9# num_nodes is set 96
num_nodes is set 100
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
[1]+  Segmentation fault      ns 100nodes-4S-24R-4M-AODV-TCP-ran-20008001.tcl
root@Mozmin-PC:/home/mozmin/NS/ns-allinone-2.35/TCL Files 9# num_nodes is set 96
num_nodes is set 100
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
PacketQueue:: remove() couldn't find target
[2]+  Exit 1                  ns 100nodes-4S-24R-4M-AODV-TCP-ran-20008001.tcl

root@Mozmin-PC:/home/mozmin/NS/ns-allinone-2.35/TCL Files 9# num_nodes is set 96
num_nodes is set 100
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!

Direction for pkt-flow not specified; Sending pkt up the stack on default.
Direction for pkt-flow not specified; Sending pkt up the stack on default.
PacketQueue:: remove() couldn't find target
[2]+  Exit 1                  ns 100nodes-4S-24R-4M-AODV-TCP-ran-20008003.tcl
```

IV. Results And Discussions

Scenario: The simulation area was kept 2000m X 800m. The number of malicious node is varied from zero to ten nodes in each group.

The throughput obtained is tabulated in Table 3 and is plotted in Figure 4 and Figure 5.

The number of packets dropped is tabulated in Table 4 and is plotted in Figure 6 and Figure 7.

The Average Latency is tabulated in Table 2 and is plotted in Figure 8.

The average latency, packet drop and network throughput under each case was extracted from the trace file and are tabulated as follows.

Table 2: Average Latency.

No. Of Malicious Nodes	Average		
	Latency	Drop	Throughput
0	0.684924423	6223	208699
4	0.7360077689	5416	198582
8	0.8784429490	6846	191392
12	0.8970458744	7380	194690
16	0.9517124875	7826	175173
20	0.8562526454	9203	189337
24	0.9325876447	7958	193179
28	0.9259584684	7143	176311
32	0.9484106399	8488	179632
36	1.074203424	9269	183430
40	1.0593209064	10506	178676

We have tabulated the average latency, drop, and throughput in the simulation time of 200 seconds against the number of malicious nodes. The graph is shown in Figure 9. The values on the y-axis are plotted on a logarithmic scale.

V. Conclusion

From the plots, we have observed that as we increase the number of malicious nodes from 0 to 40, the Average Packets Dropped is lowest with 4 malicious nodes in the system and Network Throughput is highest with 0 malicious nodes in the system. The average end to end delay of the system is lowest with 4 malicious nodes in the system.

Figure 4 and Figure 5 shows the network throughput as the number of malicious nodes was varied from 0 to 40 numbers in a network of 100 mobile nodes. The network throughput gradually increases with the simulation time giving highest throughput of 208699 bits/sec at 200th second when the number of malicious node was 0. This can be seen from the Table 3, the network throughput was 178676 bits/sec with 40 malicious node which is comparatively low.

Figure 6 and Figure 7 shows the number of control and data packets dropped. Number of packet dropped varies with the number of malicious nodes. 0 malicious node means there is no malicious node in the network. As the number of malicious node increased, we have observed that network suffers from higher packet drop compared to when the number of malicious node was kept low. With 0 malicious node, the drop was 6223 packets and with 40 malicious nodes the drop was 10506 packets.

The average end to end delay as seen in Figure 8, increases gradually as the number of malicious node increases from 0 to 40 in the network. The lowest end to end delay recorded was 0.6849 seconds with 0 malicious nodes and the highest end to end delay recorded was 1.0593 seconds with 40 malicious nodes during the simulations.

Future Work

We intend to carry out simulations with other routing protocols like DSR and TORA. Other existing performance metrics shall be studied through various simulations. As Ad hoc networks are open to both external and internal attacks due to lack of any centralized security system, we will try to make a study on Black Hole and Gray Hole attacks. These attacks are required to be analyzed on other existing MANET routing protocols. We will try to device methods of detection of selfish nodes in the Ad hoc networks and improve the performance of the network.

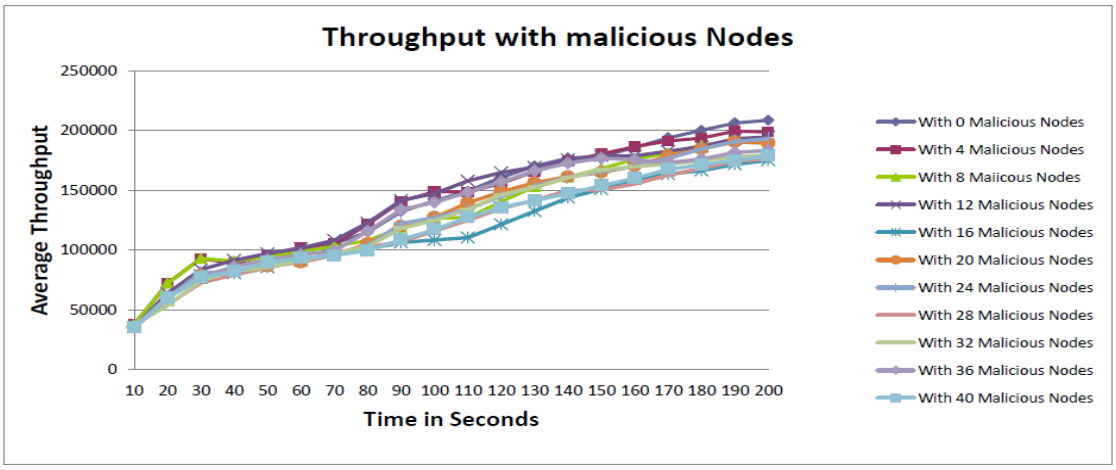

Figure 4: Network Throughput against time with malicious nodes varying from zero to ten in each group.

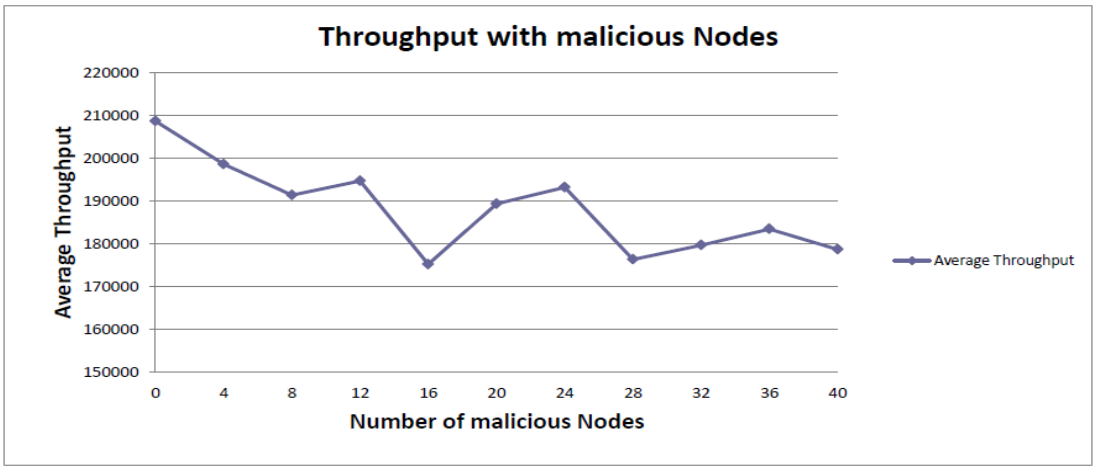

Figure 5: Network Throughput against number of malicious node with malicious nodes varying from zero to ten in each group.

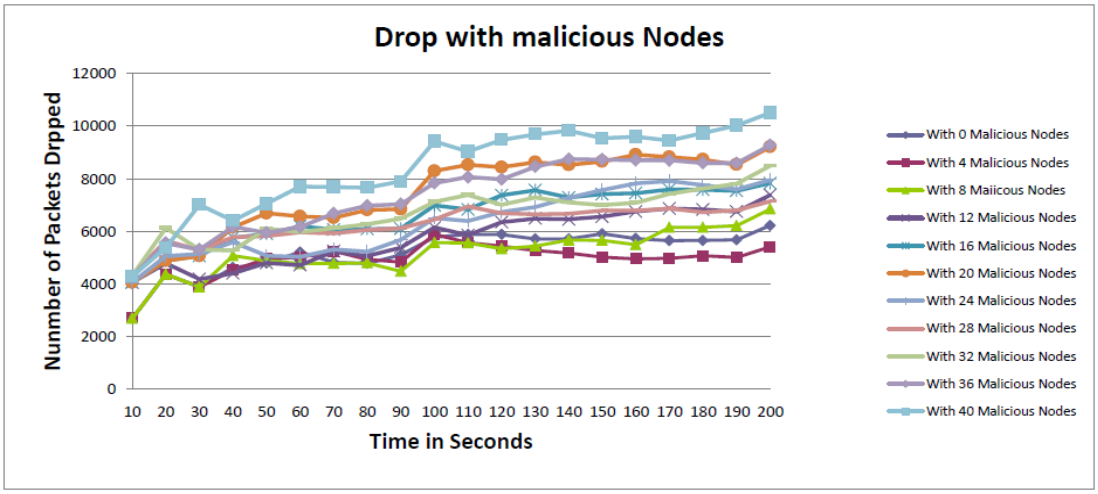

Figure 6: Number of Packets Dropped against time with malicious nodes varying from zero to ten in each group.

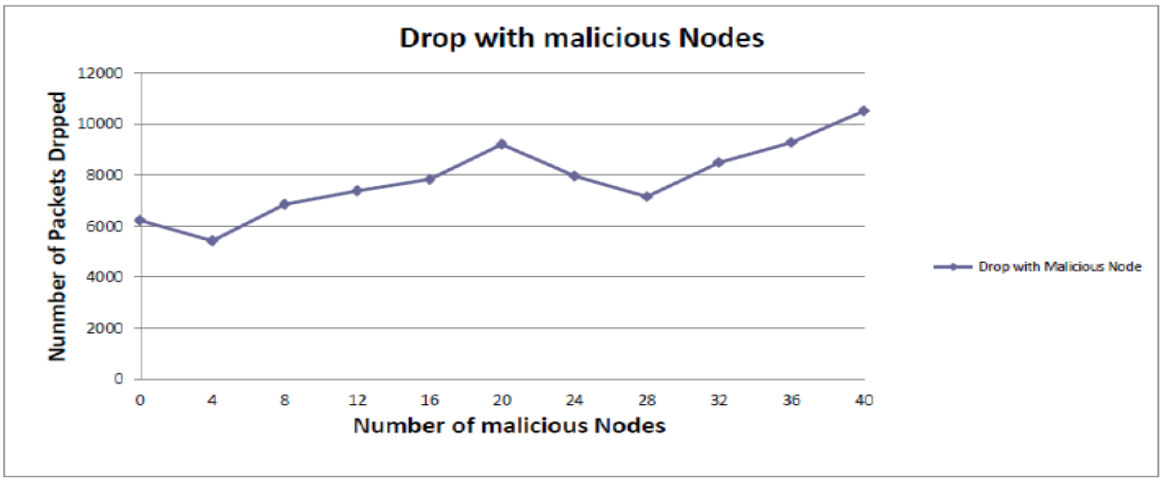

Figure 7: Number of Packets Dropped against number of malicious nodes with malicious nodes varying from zero to ten in each group.

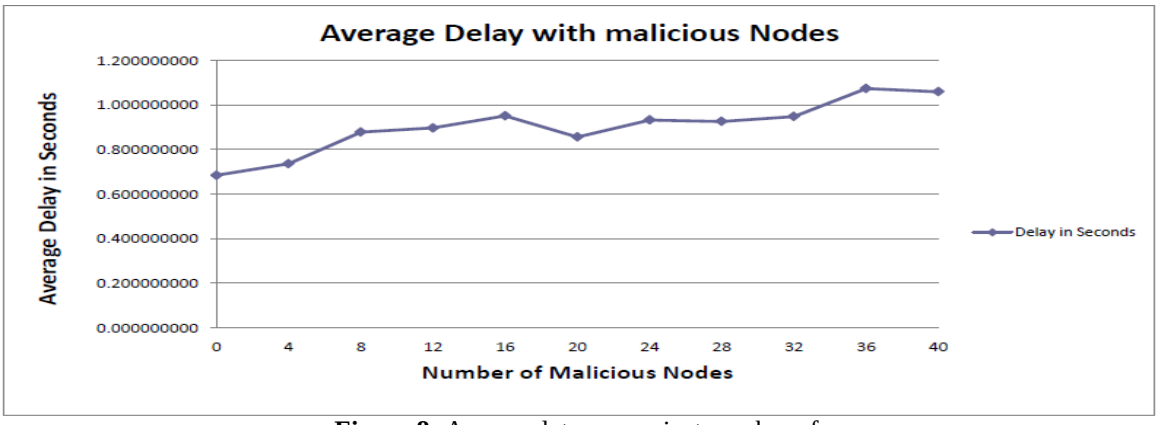

Figure 8: Average latency against number of malicious node with malicious nodes varying from zero to ten in each group.

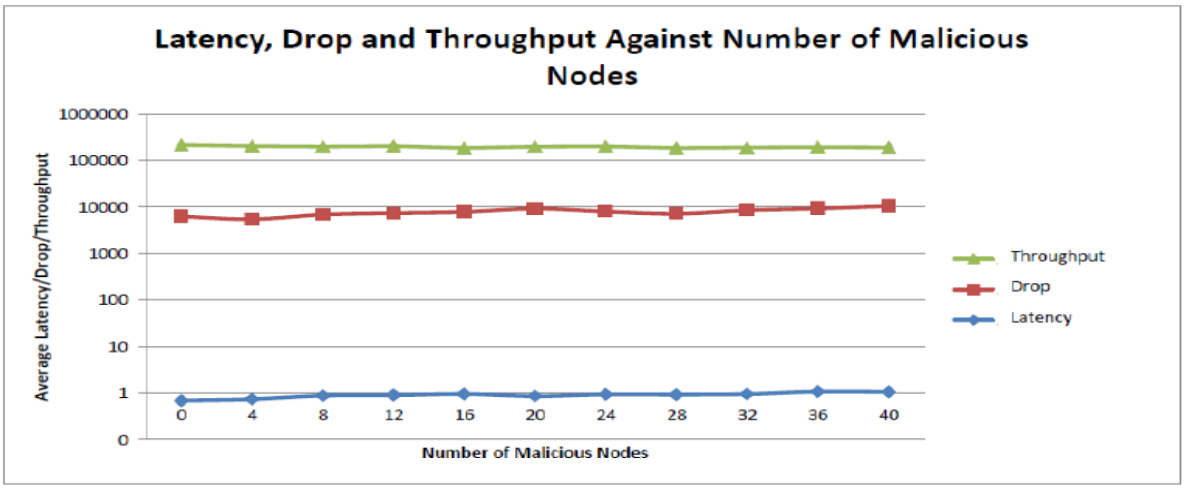

Figure 9: Average Latency, Packets Dropped and Network Throughput against number of malicious nodes.

References

[1]. Wenye Wang, Xinbing Wang, and Arne A. Nilsson, "Energy-Efficient Bandwidth Allocation in Wireless Networks: Algorithms, Analysis, and simulations".
[2]. The ns Manual (formerly ns Notes and Documentation). The Network Simulator, http://www.isi.edu/nsnam/ns
[3]. Mohammad Siraj & Soumen Kanrar, "Performance of Modeling wireless networks in realistic environment**"**.
[4]. Kurose, Ross, "How To Misuse Aodv: A Case Study Of Insider Attacks Against Ad- Hoc Routing Protocols".
[5]. Brian Russell, "Maximizing Throughput in a SimulatedWireless Environment".
[6]. Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaka Nemoto, Nei Kato, and Abbas Jamalipour, "A survey of Routing Attacks in Mobile Ad Hoc Networks".
[7]. Elmurod A. Talipov, "Adding Malicious Node to AODV".
[8]. Mozmin Ahmed and Dr. Md. Anwar Hussain, "Understanding Vulnerability of Adhoc Networks Under Malicious Node Attacks".
[9]. Mozmin Ahmed and Dr. Md. Anwar Hussain, "Effect of Malicious Node Attacks Under Practical Adhoc Network"**.**
[10]. Baruch Awerbuch, David Holmer, and Herbert Rubens , "High Throughput Route Selection in
[11]. Multi-rate Ad Hoc Wireless Networks".

APPENDIX

Table 3: Network Throughput with malicious nodes varying from zero to ten in each group.

Time	Number of Maliicous Nodes										
(Sec)	0	4	8	12	16	20	24	28	32	36	40
10	37550	37550	37550	35332	35332	35332	35332	37794	37794	35254	35136
20	72104	72104	72104	63852	60561	60561	59787	54200	53430	59514	59911
30	92797	92797	92797	83593	78740	78847	81488	72596	74529	77641	77134
40	89913	88748	90998	91392	80385	82015	81185	79294	82368	86207	82114
50	95255	95647	94267	97021	85590	86384	86589	85102	85529	91616	89886
60	100734	101975	98500	101581	90816	89598	90286	91498	91293	96121	92975
70	105431	104921	103184	108225	96597	95707	96681	97535	96968	99221	95483
80	114907	121505	107855	122783	100810	105128	103272	102687	102959	115668	99457
90	132149	140888	119061	141652	106315	119673	122297	106894	118182	133715	108572
100	141314	148908	126441	147162	108292	127320	127027	116021	124795	139856	117120
110	149329	148479	127169	157845	110314	139531	134446	124834	133854	148246	127237
120	160943	155947	140719	164956	121341	148846	144876	134795	146355	157135	135733
130	170266	165855	153067	169461	132557	156342	153631	141570	152476	166166	141358
140	177001	174579	160779	175635	143707	161297	160847	149876	160543	172702	147170
150	178382	180366	168332	178524	150966	164885	165676	150238	167050	176751	153867
160	185835	186524	175873	178729	159221	170336	169884	155227	169896	175525	160005
170	193938	191250	181185	182681	163527	178719	176680	162735	171708	173192	167493
180	200213	193540	187562	186525	166475	184582	184589	168288	174934	176102	171292
190	206348	199489	191761	193010	171598	190491	190648	174284	177955	181665	174912
200	208699	198582	191392	194690	175173	189337	193179	176311	179632	183430	178676

Table 4: Number of Packets Dropped with malicious nodes varying from zero to ten in each group

Time	Number of Maliicous Nodes										
(Sec)	0	4	8	12	16	20	24	28	32	36	40
10	2688	2688	2688	4060	4060	4060	4060	4314	4314	4290	4290
20	4365	4365	4365	4785	4882	4882	5065	5642	6125	5550	5376
30	3884	3884	3884	4184	5065	5063	5138	5283	5309	5305	7003
40	4620	4519	5074	4399	5759	6149	5587	5775	5266	6168	6399
50	4787	4962	4890	4797	5902	6686	5076	5820	6098	5944	7048
60	5213	5008	4771	4715	6197	6568	5032	5965	5972	6160	7699
70	4820	5251	4776	5241	6059	6510	5315	5918	6120	6678	7679
80	4774	4926	4802	5063	6084	6809	5221	6054	6270	6970	7660
90	5103	4826	4481	5384	6103	6842	5678	6112	6480	7031	7892
100	5774	5885	5567	6145	6982	8290	6504	6450	7117	7835	9418
110	5883	5568	5556	5849	6831	8524	6395	6936	7378	8059	9025
120	5880	5436	5333	6343	7367	8434	6738	6686	7003	7980	9475
130	5714	5270	5437	6484	7559	8626	6922	6646	7279	8452	9684
140	5715	5168	5662	6452	7284	8525	7275	6664	7092	8749	9825
150	5906	5021	5659	6552	7413	8649	7568	6792	6994	8724	9530
160	5723	4952	5491	6752	7447	8910	7824	6791	7087	8702	9591
170	5648	4979	6147	6866	7590	8822	7912	6859	7425	8696	9444
180	5653	5068	6153	6826	7574	8727	7755	6720	7625	8595	9732
190	5679	5007	6214	6746	7538	8530	7592	6801	7815	8589	10023
200	6223	5416	6846	7380	7826	9203	7958	7143	8488	9269	10506