International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 6, Issue 2 (March 2013), PP. 01-08

Performance Study of an Adhoc Network by Varying the Simulation Area and the Malicious Node Speed

Mozmin Ahmed[1], Md. Anwar Hussain[2]
[1,2]North Eastern Regional Institute of Science and Technology, Itanagar, Arunachal Pradesh, India 791109

Abstract:- We have simulated an Ad hoc network under two different scenarios; (i) varied the simulation area gradually from 400m X 160m to 2000m X 800m and, (ii) varied the malicious node speed and kept the non malicious node speed constant. The data is extracted for each simulation from the trace file using per script. From the plotted data, a study of the performance of the network with respect to the throughput and the drop is carried out. **Packet Drop** occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet drop is distinguished as one of the main error types encountered in digital communications. The **System Throughput** or aggregate throughput is the sum of the data rates that are delivered to all terminals in a network. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

Keywords:- Adhoc Network, Malicious Node, Network Simulation, Performance Study, Simulation Area, Packet Drop, System Throughput.

I. INTRODUCTION

A wireless or mobile ad-hoc network (MANET)[1] is formed by an autonomous collection of mobile users or a group of nodes which are not physically connected. The network is ad hoc because it does not integrate on an existing infrastructure, such as routers or access points. Here each node participates in routing by forwarding data for other nodes. The communication is done over a network temporarily created amongst the nodes connected within the radio range.[2] Wireless Networks faces a number of problems with respect to security solutions due to the dynamically changing topology. A wide variety of attacks can deteriorate the performance of such kind of network. A **Malicious Node** can intentionally drop some (or all) routing and data messages. As the number of packet dropping increases, the normal functioning of the network may be completely disrupted, since all the mobile nodes in a MANET behaves both as host and routers.[3] Our study is based on an Adhoc network by changing the simulation area and varying the malicious node speed. The simulation is carried out with Network Simulator NS 2.31[4] in Debian Linux 4 using AODV routing protocol.

Ad-hoc On-Demand Distance Vector (AODV) is a reactive routing protocol. It establishes a route to a destination only on demand. The most common routing protocols of the Internet are proactive, that is, they find routing paths independently of the usage. AODV maintains the routes as long as they are needed by the sources. AODV forms trees amongst the multicast group members. The trees are composed of the group members and the nodes needed to connect the members. AODV is vulnerable to various kinds of attacks as the establishment of the routes is dependent upon the co-operation amongst all the nodes in the network.

II. IMPLEMENTING AODV ROUTING PROTOCOLS

To study the effects of the presence of malicious nodes in Ad-hoc networks, two performance metrics are measured for a number of situations. These are the Network Throughput and the Average Packet Drop. Each simulation scenario consists of 100 nodes, divided into four groups with twenty-five members each. Out of these twenty-five members, one node acts as a sender node and rest twenty-four nodes behaves as receivers. All the nodes are free to move in any quadrant and the nodes moves from the initial position to the final position in a straight line. The speed of all the nodes is defined for uniform movement. The simulation time is kept at 200 seconds for all the simulations.

In the first scenario, different simulation spaces used are 400m X 160m, 800m X 320m, 1200m X 480m, 1600m X 640m and 2000m X 800m. Under each simulation area, the node speed is varied from 1m/sec to 10m/sec. For this scenario, we assume the nodes in an ideal situation with no malicious activity.[5]

In the second scenario, we have carried out the simulation of 100 nodes in a space of 2000m X 800m. One amongst these twenty-four node is programmed to behave maliciously in each group. Thus there are four malicious nodes in our simulation model. The malicious node drops every packet it receives instead of forwarding it to the destination or for onward transmission. The non-malicious node speed is varied from 1m/sec

to 10m/sec. For all the cases, the malicious node speed is kept same, doubled and halved with respect to the non-malicious node speed. The node positions are randomly generated for the initial and final position to give the network a realistic view[6].

The result for the simulations under the above scenarios is extracted from the trace file using perl script file[7]. The average throughput[8] is calculated by adding the number of packets transmitted from all nodes and averaged over the time of simulation. Similarly, the average packet dropped[9] is calculated by adding the total packets dropped by the nodes and averaged over the simulation period. The data obtained is tabulated and plotted and a comparative study is done.

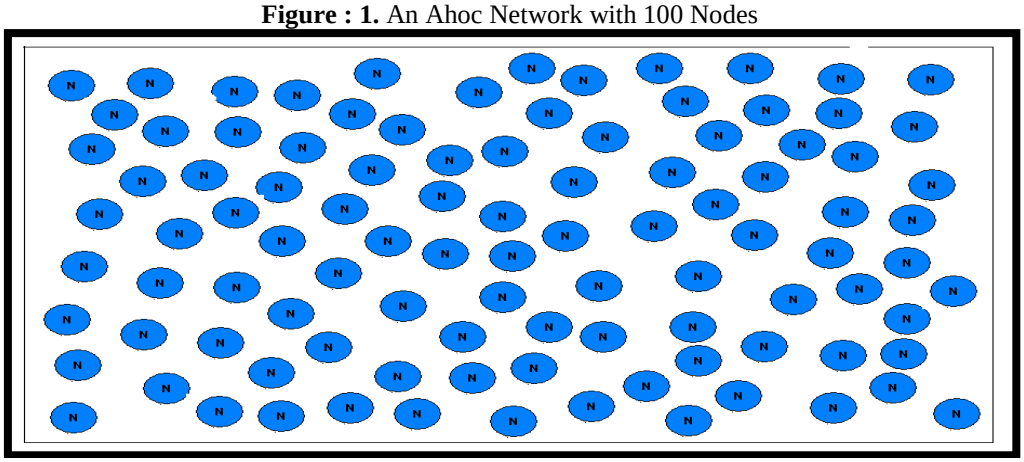
III. SIMULATIONS, RESULTS AND ANALYSIS

PARAMETERS	VALUE	
	SCENARIO 1	SCENARIO 2
SIMULATOR	NS-2, VERSION 2.31	NS-2, VERSION 2.31
SIMULATION TIME	200 SECONDS	200 SECONDS
NUMBER OF NODES	100	100
CHANNEL TYPE	WIRELESS	WIRELESS
MAC TYPE	802.11	802.11
ROUTING PROTOCOL	AODV	AODV
TRANSPORT LAYER PROTOCOL	TCP	TCP
TRAFFIC MODEL	FTP	FTP
DATA PACKET SIZE	64 BYTES	64 BYTES
NUMBER OF CONNECTIONS	96	96
SPEED	1M/SEC TO 10M/SEC	1M/SEC TO 10M/SEC
NUMBER OF MALICIOUS NODES	NIL	4
TOPOLOGY	400M X 160M, 800M X 320M, 1200M X 480M, 1600M X 640M, 2000M X 800M	2000M x 800M

Table I : AODV Scenario Parameters.

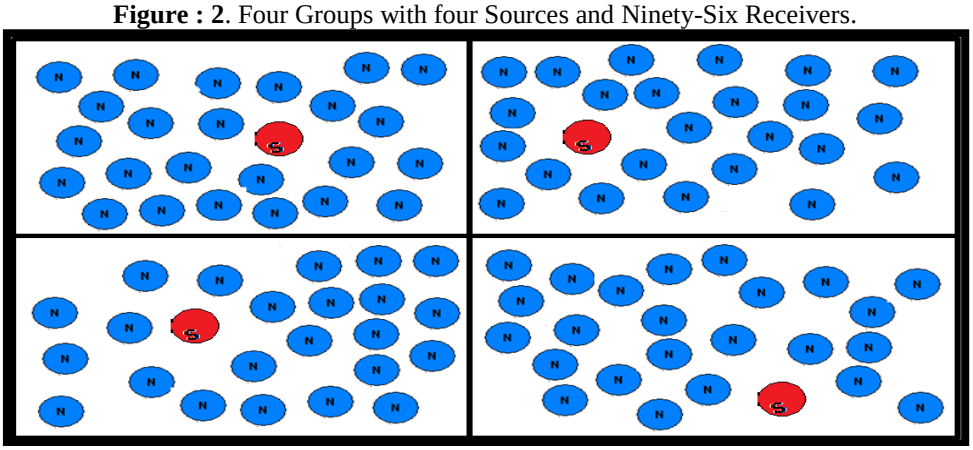
A wireless network with hundred mobile nodes is created. The initial (starting) positions of the nodes are randomly oriented in a pre-defined space. The nodes are programmed for linear movement towards final destined position, which are also randomly defined. The nodes are arranged in the fashion as shown in the figure 1.

Figure : 1. An Ahoc Network with 100 Nodes



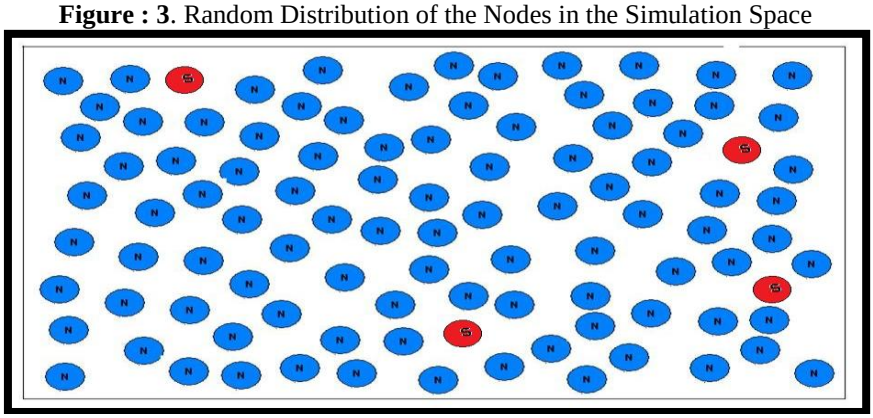
SCENARIO 1 : This is an ideal situation without any malicious nodes in the network. All the hundred nodes in the scenario are divided into four groups with twenty-five members each. The simulation spaces selected are 400m X 160m, 800m X 320m, 1200m X 480m, 1600m X 640m and 2000m X 800m. The nodes with red colour are the source nodes, and the nodes with blue colour are the receiver nodes. Figure 2 show the schematic distribution of the nodes in the network.

Figure : 2. Four Groups with four Sources and Ninety-Six Receivers.



Here all the nodes are free to move in any quadrant, within the defined space. The figure 3 shows the real time distribution of the nodes in random position.

Figure : 3. Random Distribution of the Nodes in the Simulation Space



In this scenario, simulations are carried out by changing the space. Under each simulation area we varied the node speed from 1m/sec to 10m/sec. The results from each simulation is extracted from the trace files.

The average throughput is calculated using the perl script file. The number of bits transmitted from all the nodes are added and averaged over the time of simulation. The data obtained is tabulated in Table II and the graph is plotted in Figure 4.

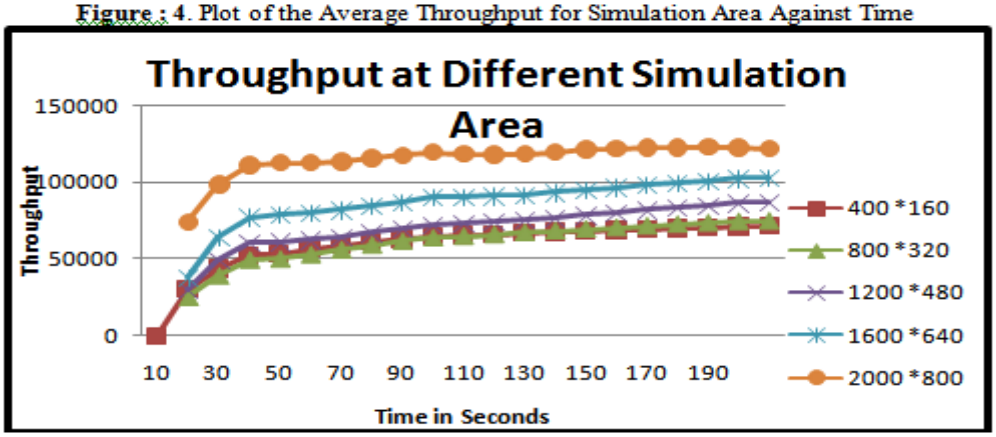
Time	**Throughput at Different Simulations Areas (sq.m)**				
	400 *160	**800 *320**	**1200 *480**	**1600 *640**	**2000 *800**
In Secs	**In bits per seconds**				
10	30351	24597	29910	37391	74496
20	43609	38662	49196	63954	98543
30	52406	49070	60593	76746	110529
40	53516	49671	60969	78908	112345
50	56432	52636	62195	79863	112586
60	59078	55720	64187	81567	113080
70	61409	58821	66708	84022	115448
80	63133	61291	69320	86883	117245
90	64568	63589	72173	89689	119237
100	65182	64672	72947	90171	118019

110	65937	65776	73979	90615	117425
120	66768	67061	75304	91545	117966
130	67504	68183	76698	92821	119214
140	68171	69267	78359	94494	120794
150	68805	70362	80047	96229	121775
160	69412	71447	81701	97711	122056
170	69985	72441	83197	99276	122198
180	70532	73372	84747	100799	122347
190	71045	74251	86036	102173	122194
200	71366	74619	86515	102524	121337

Table II : Average Throughput At Different Simulation Areas**.**

Figure : 4. Plot of the Average Throughput for Simulation Area Against Time

Figure : 4. Plot of the Average Throughput for Simulation Area Against Time

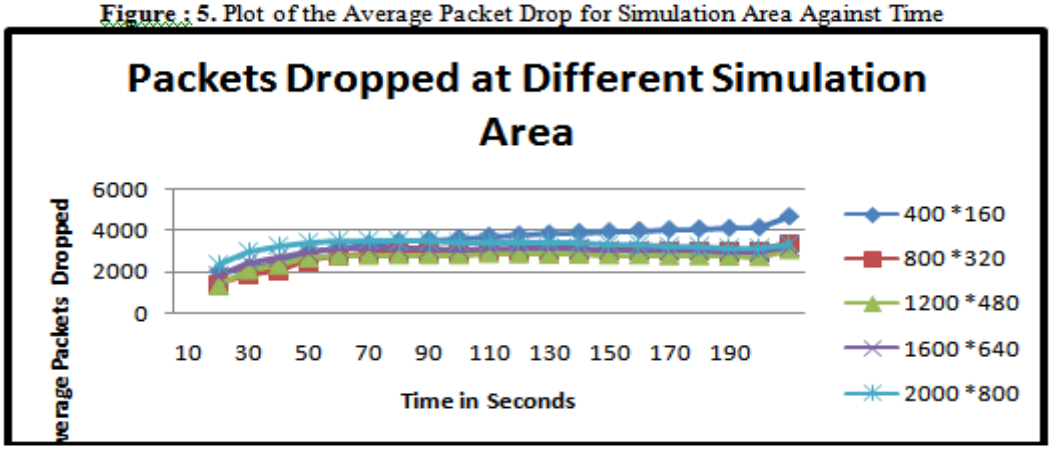


The average packets drop is calculated using the perl script file. The total number of packets dropped from all the nodes are added and averaged over the time of simulation. The data obtained is tabulated in Table III and the graph is plotted in Figure 5.

Time	**Packets Dropped at Simulations Area (sq. m)**				
	400 *160	**800 *320**	**1200 *480**	**1600 *640**	**2000 *800**
In Secs					
10	1983	1440	1341	1768	2337
20	2193	1867	2098	2437	2952
30	2406	2027	2355	2678	3204
40	2934	2543	2677	2902	3380
50	3181	2757	2788	3084	3470
60	3340	2851	2822	3091	3480
70	3463	2939	2831	3115	3459
80	3539	2985	2839	3099	3459
90	3613	2962	2829	3074	3411
100	3716	3032	2895	3137	3431
110	3774	3034	2872	3129	3432
120	3838	3036	2866	3124	3406
130	3895	3041	2862	3096	3358
140	3942	3025	2844	3071	3315
150	3986	3022	2828	3049	3279
160	4031	3012	2802	3011	3218
170	4067	2996	2788	2985	3174
180	4097	2986	2771	2953	3128
190	4135	2975	2752	2933	3095
200	4666	3351	3077	3210	3316

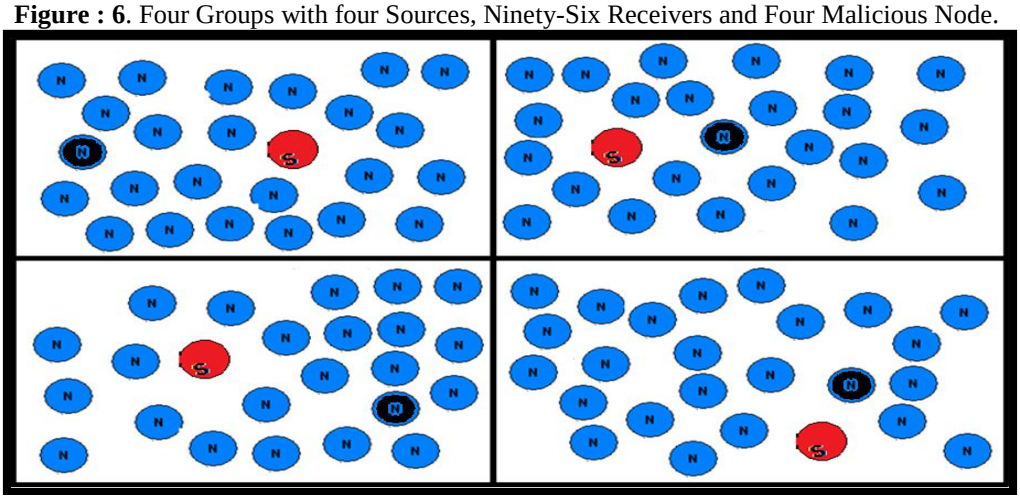
Table III : Average Packet Drop At Different Simulation Areas

Figure : 5. Plot of the Average Packet Drop for Simulation Area Against Time



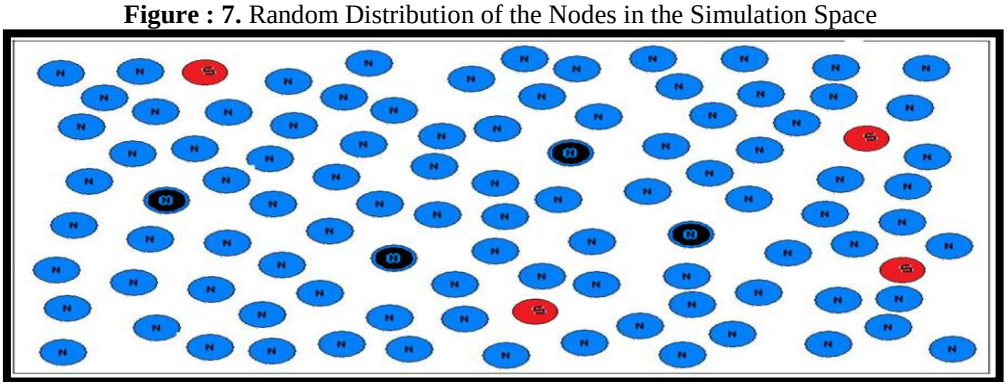
SCENARIO 2 : Here, in the simulation Area of 2000m X 800m, we have divided the nodes in four groups of twenty-five members each. The nodes with black colour are the malicious nodes, the nodes with red colour are the source nodes, and the nodes with blue colour are the receiver nodes. Figure 6 show the schematic distribution of the nodes in the network.

Figure : 6. Four Groups with four Sources, Ninety-Six Receivers and Four Malicious Node.



All the nodes are free to move in any quadrant, within the defined space. The figure 7 shows the real time distribution of the nodes in random position.

Figure : 7. Random Distribution of the Nodes in the Simulation Space



In this scenario, simulations are carried out by varying the speed of the non-malicious nodes from 1m/sec to 10m/sec for each case. Corresponding to the speed of the non-malicious nodes, the malicious node

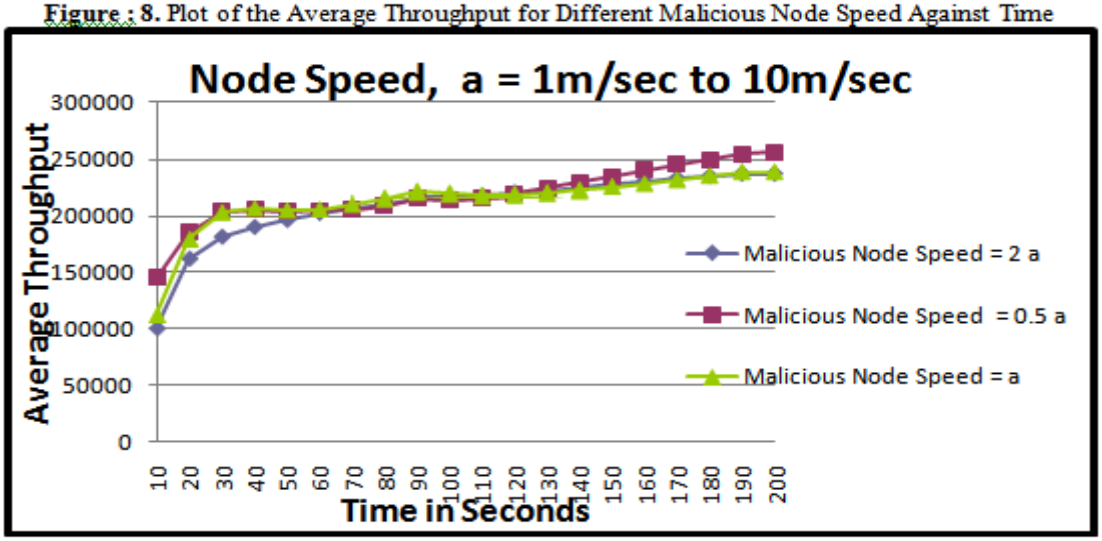
speed was kept same, doubled and halved to study the network behaviour. The results from each simulation is extracted from the trace files.

The average throughput is calculated using the perl script file. The number of bits transmitted from all the nodes are added and averaged over the time of simulation. The data obtained is tabulated in Table IV and the graph is plotted in Figure 8. In the Table IV, the variable 'a' represents the speed of the non-malicious nodes which varies from 1m/sec to 10m/sec.

Time	Throughput at Malicious Node Speed (m/Sec)		
	2a (Doubled)	0.5a (Halved)	a (Same)
In Sec	In bits per second		
10	100695	144609	112654
20	162906	185808	180192
30	182359	204274	204060
40	191127	206025	207559
50	197367	204050	205944
60	203646	204680	206760
70	208589	206267	210996
80	212262	208602	215832
90	217384	215059	221753
100	217085	214415	220069
110	217790	215157	218218
120	220449	219687	219279
130	222035	224550	220660
140	225613	229163	222803
150	228493	233910	225874
160	230838	240266	228198
170	233060	245311	231434
180	235064	250057	235091
190	237120	254566	238684
200	237053	256252	238645

Table IV : Average Throughput At Different Malicious Node Speed

Figure : 8. Plot of the Average Throughput for Different Malicious Node Speed Against Time

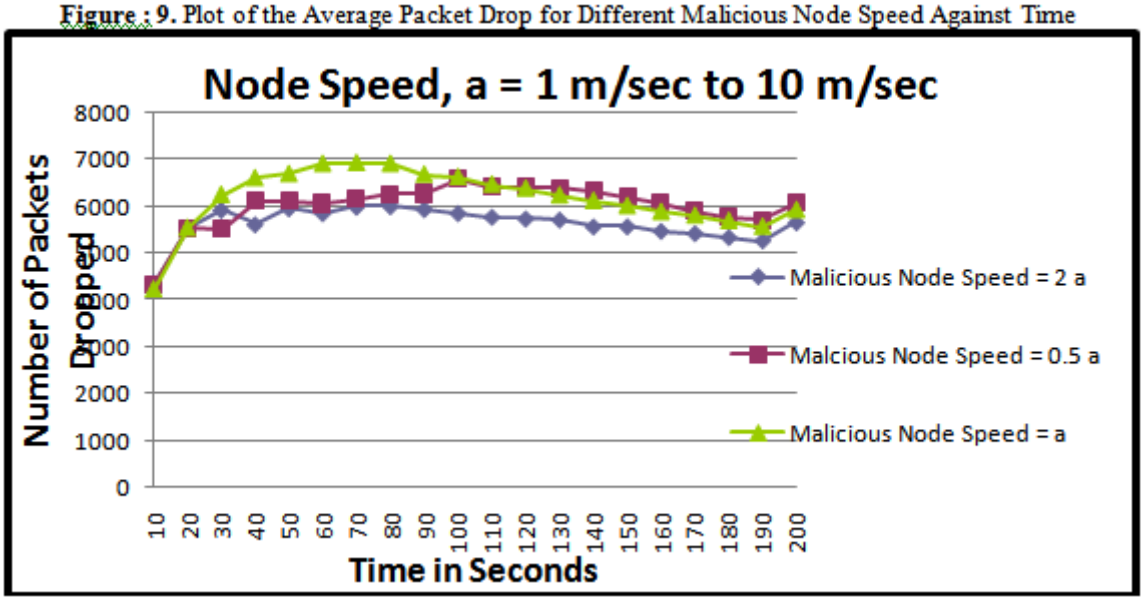


The average packets drop is calculated using the perl script file. The total number of packets dropped from all the nodes are added and averaged over the time of simulation. The data obtained is tabulated in Table V and the graph is plotted in Figure 9. In the Table V, the variable 'a' represents the speed of the non-malicious nodes which varies from 1m/sec to 10m/sec.

Time	Packet Dropped at Malicious Node Speed (m/Sec)		
	2a (Doubled)	0.5a (Halved)	a (Same)
In Sec			
10	4361	4354	4243
20	5534	5547	5556
30	5926	5528	6267
40	5612	6125	6621
50	5959	6145	6710
60	5853	6069	6928
70	5994	6168	6942
80	6008	6277	6929
90	5943	6281	6700
100	5856	6599	6644
110	5775	6443	6487
120	5735	6414	6399
130	5715	6408	6256
140	5566	6328	6138
150	5571	6202	6027
160	5470	6085	5900
170	5421	5912	5823
180	5338	5788	5709
190	5266	5720	5584
200	5656	6087	5942

Table V : Average Packet Drop At Different Malicious Node Speed

Figure : 9. Plot of the Average Packet Drop for Different Malicious Node Speed Against Time



IV. CONCLUSION

In this paper, all the results shows the performance of an Adhoc Network depends on many factors such as the network space, malicious behaviour of the nodes, speed of the malicious nodes, in comparision with the non malicious node speed.

The efficiency of an Adhoc Network with respect to the system throughput and the number of packets loss is dependent on the Simulation Area and the Node Speed. The throughput of the system increases with the increase in the simulation area. The packets dropped for smaller simulation area is high. It gradually reduces and, at bigger simulation areas, the drop again increases.

Our simulation result ensures that malicious nodes give a bad impact on the performance of AODV from the point of view of throughput and packets dropped. We also note that the operation of the malicious node is dependent on the mobility. It is observed that with increase in the malicious node speed in the network, the throughput of the system increases, and the average drop of the system reduces.

V. FUTURE WORK

We propose to extended this work in reverse way, by keeping the malicious node speed constant and varying the non-malicious node speed. The will lead to understanding of the network in the varied nature. Also a study can be carried out on the latency (Average Delay) of the system which may be affected by the various factors mentioned above.

A Study can be done to calculate the average latency and throughput of the system by introducing and gradually increasing the number of malicious nodes in the Adhoc Network.

Security is an essential requirement in Wireless Adhoc Network due to the nature of mobility and open media as compared to those in the traditional Wired Network. In future, we would try to detect the threats and find some affective solutions to protect the Wireless Adhoc Networks from all kinds of security risks.

REFERENCES

[1]. "Search on Survivability of Mobile Ad-hoc Network". – Yuan Zhou, Chunhe Xia, Haiquan Wang and Jianzhong Qi.

[2]. " Performance of Modeling wireless networks in realistic environment**"-** Mohammad Siraj & Soumen Kanrar.

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

[4]. The *ns* Manual (formerly *ns* Notes and Documentation). The Network Simulator, http://www.isi.edu/nsnam/ns

[5]. "Effect of Space in an Adhoc Network" – Mozmin Ahmed and Md. Anwar Hussain.

[6]. "Understanding Vulnerability of Adhoc Networks under Malicious Node Attacks"- Mozmin Ahmed and Md. Anwar Hussain.

[7]. "TCP Performance Simulation Using NS-2" – Johanna Antila.

[8]. " Performance of TCP-Throughput on NS-2 by Different Simulation Parameters" – Neeraj Bhargwa, Ritu Bhargawa, Anchal Kumawat and Bharat Kumar.

[9]. "Modelling Delay and Packet Drop in Networked Control Systems Using Netwrok Simulator NS2" – Mohammad Sahidul Hassan, Christoper Harding, HongnianYu and Alison Griffiths.