AGENT BASED INTRUSION DETECTION SYSTEM IN MANET

J. K. Mandalr*, Khondekar Lutful Hassan#

*University of Kalyani, Kalyani,
Nadia-741235, West Bengal, India,
#A.K.C. School of I.T
University of Calcutta
Kolkata, West Bengal, India
{ jkm.cse@gmail.com, klhassan@yahoo.com }

ABSTRACT

In this paper a technique for intrusion detection in MANET has been proposed where agents are fired from a node which traverses each node randomly and detect the malicious node. Detection is based on triangular encryption technique (TE) where AODV is taken as routing protocol. For simulation we have taken NS2 (2.33) where two type of parameters are considered out of which number of nodes and percentage of node mobility are the attributes. For analysis purpose 20, 30, 30, 40, 50 and 60 nodes are taken with a variable percentage of malicious node as 0 %(no malicious), 10%, 20%, 30% and 40%. Analysis have been done taking generated packets, forwarded packets, delay, and average delay as parameters

KEYWORDS

Agent Based Intrusion Detection System (AIDS), MANET, NS2, AODV, Mobile Agent.

1. INTRODUCTION

As MANET is infrastructure less, has the node mobility and it is distributed in nature, every node act as router. So security is the main challenge in MANET [1][2][3]. Many researchers have proposed and implemented different techniques for intrusion detection. Intrusion detection requires cooperation among nodes. Intrusion detection is the automated detection and subsequent generation of an alarm to alert the security apparatus at a location if intrusions have taken place or are taking place. An intrusion detection system (IDS)[4] is a defense system, which detects hostile activities in a network and then tries to prevent such activities that may compromise system security. Intrusion detection systems detect malicious activity by continuously monitoring the network. In other words, intrusion detection is a process of identifying and responding to malicious activity targeted at computing and networking resources. IDSs implemented using mobile agents is one of the new paradigms for intrusion detection. Mobile agents are special type of software agent, having the capability to move from one host to another.

Jan Zizka (Eds) : CCSIT, SIPP, AISC, PDCTA - 2013
pp. 201–208, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3622

Based on the sources of the audit information used by each IDS, the IDSs may be classified into

Host-base IDSs: In this model IDS detects attack against a single host. IDS get audit information from host audit trails.

Distributed IDSs. In this model, an IDS agent runs at each mobile node and performs local data collection and local detection, whereas cooperative detection and global intrusion response can be triggered when a node reports an anomaly

Network-based IDSs: In this model IDS detects attack in network,. System uses network traffic as audit information source Mobile agent is a software agent which can move through the network from host to host. For a large scale network it can move to the node and collect the audit data, and information and can perform the specific task to the designation.

In this paper A Novel Technique for Intrusion Detection System has been proposed in MANET. An agent has been triggered randomly from a node which traverses all nodes sequentially one after another till the end of nodes associated with the cell in a round. It computes the security parameters and finds the conflicted activities if any which reported as malicious activities of the node.

Section II of the paper deals with the proposed detection technique. Simulation environment has been presented in section III. Section IV deals with results and simulations. Conclusion is drawn in section V and conclusion is given at end.

2. PROPOSED TECHNIQUE

The In proposed method AODV [1, 2, 3, 8] is taken as routing protocol. A mobile agent triggered from a node of the network traverse all nodes intern one after another, monitor the activity of the nodes for its malicious behavior if exist, detect the node as malicious through an agent termed as 'Idect'. As security measure each node computes some information as source information of the node through an agent at triggering nodes followed by encryption using an algorithm called Triangular Encryption [TE][9,10] and encapsulate the information within the packet which traverse in the network. On the other hand the agent 'Idect 'randomly triggered its process of detection in randomly selected node compute the information, decode the encrypted information and compare for authentication. If this authentication fails, the node is detected as malicious and the information is forwarded to its neighbors accordingly. The detection of malicious node is guided through an encryption process where various parameters of nodes normally affected through intrusion are taken as input and a triangular based encryption is done in of these parameters to capsule the parameters in each node. The process of encryption is described is as follows. Consider a block $S= s^0_0\ s^0_1\ s^0_2\ s^0_3\ s^0_4\ s^0_5$ .... $s^0_{n-2}\ s^0_{n-1}$ of size n bits , where $s^0_1 = 0$ or 1 for 0<=i<=(n-1).Starting from MSB (s^0_0) and the next to MSB (s^0_1), bits are pair-wise XNOred, so that the first intermediate sub-stream $S^{1\,=}\ S= s^1_0\ s^1_1\ s^1_2\ s^1_3\ s^1_4\ s^1_5$ .... $s^1_{n-2}\ s^1_{n-1}$ is generated consisting of (n-1) bits, where $s^1_j = s^0_j$ (XNOR) s^0_{j+1} for 0<=j<=n-2.The first intermediate sub stream S^1 is also pair-wise XNORed to generate $S^2=s^2_0\ s^2_1\ s^2_2\ s^2_3\ s^2_4\ s^2_5\ldots\ s^2_{n-2}\ s^2_{n-1}$, which is the second intermediate sub-stream of length (n-2). This process continues (n-1) times to ultimately generate $S^{n-1}=S^{n-1}_0$, which is a single bit only. Thus the size of the first intermediate sub-stream is one bit less than the source sub-stream; the size of each of the intermediate sub-stream starting from the second one is one bit less than that of the sub-stream wherefrom it was generated; and finally the size of the final sub-stream. Figure 1 shows the generation of the intermediate sub-stream $S^{j+1} = s^{j+1}_0\ s^{j+1}_1\ s^{j+1}_2\ s^{j+1}_3\ s^{j+1}_4\ s^{j+1}_5 \ldots\ s^{j+1}_{n-(j+2)}$ from the previous intermediate sub-stream $S^j = s^j_0\ s^j_1\ s^j_2\ s^j_3\ s^j_4\ s^j_5 \ldots\ s^j_{n-(j-1)}$. The formation of the triangular shape for the source sub-stream $S= s^0_0\ s^0_1\ s^0_2\ s^0_3\ s^0_4\ s^0_5 \ldots\ s^0_{n-2}\ s^0_{n-1}$ is shown in figure 1.

$$S= s^0_0\ s^0_1\ s^0_2\ s^0_3\ s^0_4\ s^0_5 \ldots\ldots\ldots\ldots\ldots\ldots\ s^0_{n-2}\ s^0_{n-1}$$
$$S^1 = s^1_0\ s^1_1\ s^1_2\ s^1_3\ s^1_4 \ldots\ldots\ldots\ldots\ s^1_{n-2}$$
$$S^2= s^2_0\ s^2_1\ s^2_2\ s^2_3 \ldots\ s^2_{n-3}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s^{n-2} = s^{n-2}_0\ s^{n-2}_1$$
$$S^{n-1}= s^{n-1}_0$$

Fig.1. formation of triangle in TE

On generating this triangle various possibilities are there to encode. For the propose of the present scheme, all MSBs are taken in order including source bit to form the encrypted bit. This process is applied to various sensitive parameters of a node where attack may occur and the same are encapsulated for detection by the agent 'Idect'. When the agent triggered on a node for intrusion detection, it will take values of same parameters from the node under scanner and again encrypt the parameters using Triangular Encryption (TE)[9,10] through same option of encryptions. Then it compared the values of encrypted parameters with the encapsulated parameters for authentications. If the encapsulate parameters and computed parameters obtained by 'Idect' are matched then the node is nonmalicious otherwise it designate the node as malicious and mark the node accordingly. The graphical view of an ideal 'Idect' is given in figure 2.

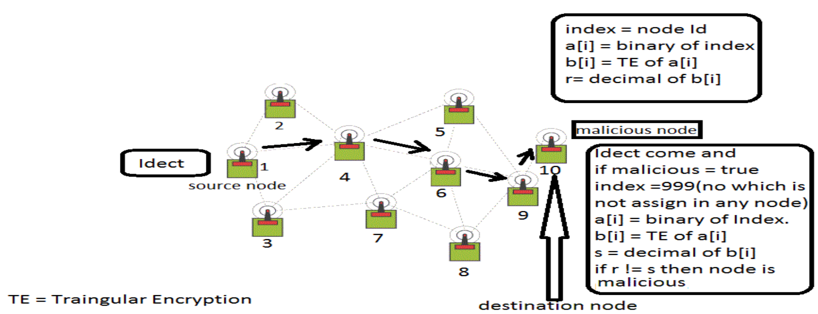

Fig. 2. Graphical view of IDS technique

3. SIMULATION ENVIRONMENT

Network Simulator 2 (NS2.33) [6][7] is taken as a tool for simulation purpose. The Network Simulator 2 is a tool of discrete event simulation in the network, and capable of simulating various types of networks. NS2 [6, 7] consists of two languages, C++ and Otcl. C++ defines the internal mechanism of the simulation object, and Otcl set up simulation by assembling and configuring objects as well as scheduling discrete events. To simulate NS2, a (.tcl) script file is required. After simulation it creates two types of file, one is trace file (tr) and another is (.nam) file. Trace file is used for calculation and statistical analysis, and that of .nam file is used to visualize the simulation process.

4. SIMULATIONS AND RESULTS

For the purpose of simulation five parameters are taken as common in each case. These are given in table 1.

Table 1: Parameter (fixed) of the simulation in 'Idect'

Routing protocols	AODV
Percentage of node mobility	40 %
Maximum packets in IFQ	50
Speed of the nodes	100 m/s
Time of simulation	10 sec

Variable parameters are

i. Number of nodes (20, 30, 40, 50, 60)
ii. Percentage of malicious node (0%,10%, 20%, 30% 40%)

Snapshot of simulation output is given in figure 3 where outputs of various parameters are shown in details

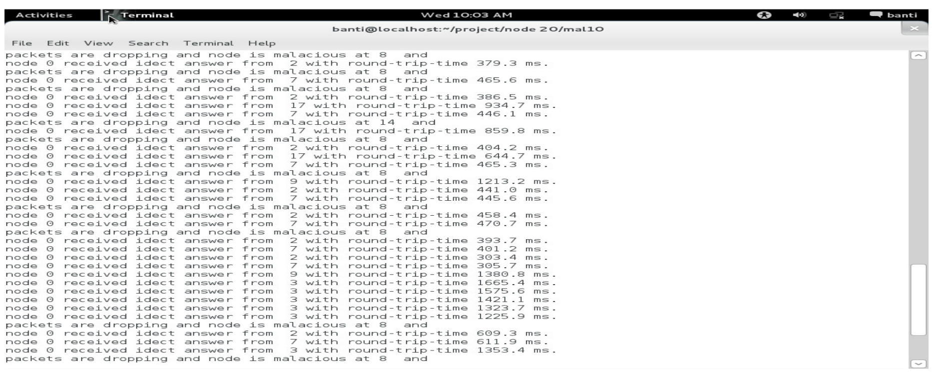

Fig. 3. Snapshot of simulation in terminal

Comparison of performance is measured with the following parameters.

A. Generated packets.
B. Forward packets.
C. Average delay.
D. Drop packets.

Results are taken considering the variable parameter like number of nodes, and percentage of malicious node. Numbers of nodes are taken 20, 30, 40, 50 and 60. And percentage of node mobility is taken as 0%, 10%, 20%, 30%, and 40%.

A. Generated of packets
   Comparison of generated packets is given table 2 and figure 4.

Table 2. Generated packets through simulation of ‘Idect’

Percentage of Malicious	Node 20	Node 30	Node 40	Node 50	Node 60
0%	1837	2218	4110	4967	6360
10%	1735	2204	4110	5126	6518
20 %	1453	2064	3622	4780	6391
30 %	644	2132	4144	4847	6871
40 %	1287	6568	6568	6568	6568

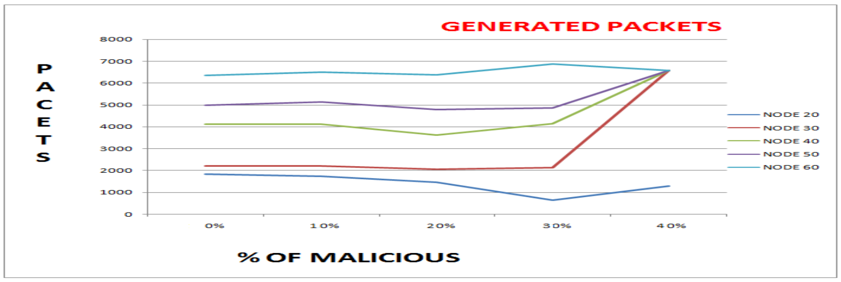

Fig.4. Comparison of number of generated packets

From table 2 and figure 4 it is seen that when the percentage of malicious node is increased, the rate of packet generation is increased. When 40 % nodes are malicious the packet generation is maximum.

B. Forward packets

Comparison of generated packets is given table 3 and figure 5 from where it Is seen that when number of malicious node is increasing number of forwarded packets are decresing.

Table 3. Number forward packets in “Idect’

Percentage of Malicious	Node 20	Node 30	Node 40	Node 50	Node 60
0	895	572	1129	377	338
10	861	405	2129	297	356
20	574	402	684	212	356
30	86	347	862	215	125
40	428	402	349	109	79

Fig.5 Comparison of forward packets

That is, rate of forwarding packets are decreasing with the increasing of percentage of malicious node. When 20 nodes are taken for simulation with 10% malicious the system behaves abnormally.

C. Average Delay

Comparison of Average Delray is given in the table 4 and figure 6 from where it is clear that delay is decreasing on increasing number of nodes as well as malicious nodes.

Table 4. Average delay (sec) in Simulations of 'Idect'.

Percentage of Malicious	Node 20	Node 30	Node 40	Node 50	Node 60
0	0.686839	0.419547	0.572877	0.272646	0.351286
10	0.302901	0.256601	0.572877	0.226283	0.344115
20	0.47166	0.281686	0.227599	0.180511	0.3649
30	0.600703	0.258949	0.424504	0.238707	0.105786
40	0.273356	0.283779	0.260255	0.329716	0.320199

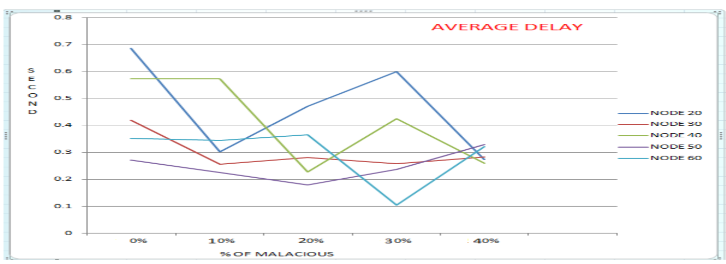

Figure 6 Comparison of Avg. delay (sec.)

From table 4 and figure 6 we can see that behavior of graph is abnormal here. It may be for node mobility because 40% nodes are moving with the speed of 100m/s, and as well as for other parameters.

D. Drop packets

Comparison of Drop Packets is given in the table 5 and figure 7.

Table 5. Number of drop packets in 'Idect'

Percentage of Malicious	Node 20	Node 30	Node 40	Node 50	Node 60
0	2314	3881	5835	8454	11748
10	2364	4083	5835	8767	11678
20	2463	4087	6246	8732	11706
30	2195	4105	6332	8788	12581
40	2555	4066	8387	8821	12483

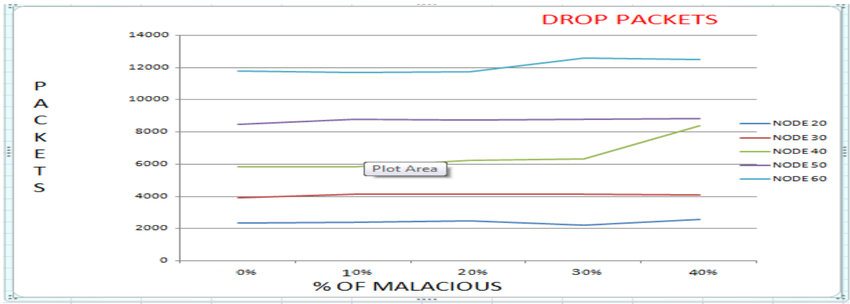

Figure 7. Comparison graphs of drop packets in 'Idect'.

From the above table 5 and figure 7 we can see that rate of drop packets are increasing with respect to percentage of malicious node. The rates of drop packets are slightly increasing because AODV broadcast packets are drop rapidly at every node due to node mobility. Source node is sending packets very fast to other nodes so it is unable to control all the packets, as a result maximum packets are drop at source node.

5. CONCLUSIONS

In this paper we have introduced a method and technique to detect malicious node using mobile Agent ('Idect'). Compare and analysis of the performance at various parameters in AODV routing protocol are also done extensively. It is seen from the simulation that in some cases the network behave abnormally. The reason of abnormality is due to 40 % nodes are moving with high speed (100m/s). Only source node is firing the secure agent 'Idect' to every node with a high frequency so it is unable to control all the packets, as a result it drop many packets. The technique proposed are very simple for detection of malicious node as the 'Idect' agent visit all nodes randomly across all nodes of the network irrespective of the topologies and thus it is an agent based intrusion detection system.

ACKNOWLEDGMENTS

The authors expressed deep sense of gratuity towards the Dept of CSE University of Kalyani and the PURSE Project of DST, Govt. of India, from here the computational recourses are used for the research..

REFERENCES

[1] C.Siva Ram Murthy and B.S manoj" Ad Hoc Wireless networks architecture and protocols" Pearson education india 2005.
[2] Prasant Mohapatra, Srikanth Krishnamurthy "Ad hoc networks: technologies and protocols" Springer 2005
[3] Chai-Keong Toh "Ad hoc mobile wireless networks: protocols and systems " Prentice Hall.
[4] Amitava Mishra "Security and Quality of Service in Adhoc Wireless Network", Cambridge University Press .
[5] Sarkar, S.K., Basavaraju, T.G., Puttamadappa, C.: Ad hoc Mobile Wireless Networks: Principles, Protocols and Applications. Auerbach Publications (2008)
[6] Teerawat Issariyakul, Ekram Hossain "Introduction to Network Simulator NS2" Springer (2009)
[7] Marc Greis' Tutorial http://www.isi.edu/nsnam/ns/tutorial/

[8] Mubashir Husain Rehmani, Sidney Doria, and Mustapha Reda Senouci “A Tutorial on he Implementation of Ad-hoc On Demand Distance Vector (AODV) Protocol in Network Simulator (NS-2)”

[9] Mandal, J. K.,Dutta, S.,Mal, S., “A Multiplexing Triangular Encryption Technique – A Move Towards Enhancing Security in E-Commerce, Proc. of Conference of Computer Association of Nepal, December, 2001.

[10] Mandal, J. K., Chatterjee R, “Authentication of PCSs with Triangular Encryption Technique”, Proceedings of 6th Philippine Computing Science Congress(PCSC 2006), Ateneo de Manila University, Manila, Philippine, March 28-29,2006.

[11] Dokurer, S. Ert, Y.M. ; Acar, C.E.” Performance analysis of ad-hoc networks under black hole attacks”, Proceedings. IEEE. pp. 148 – 153, 2007

[12] Perkins, C.E., Royer, E.M., "Ad-hoc on-demand distance vector routing" ,www.cs.ucsb.edu/~ravenben/classes/papers/aodv-wmcsa99.pdf

[13] Deng, H., Li, W., Agrawal, D., "Routing Security in Wireless Ad Hoc Networks" IEEE Communication Magazine (October 2002) pp. 70-75

[14] Al-Shurman, M., Yoo, S., Park, S., "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference (2004) pp. 96-97

[15] Mishra, A., Nadkarni, K., Patcha, A., "Intrusion detection in wireless ad-hoc networks", IEEE Wireless Communications, February 2004, pp. 48-60.