A NOVEL TECHNIQUE TO DETECT INTRUSION IN MANET

J. K. Mandal [1] and Khondekar Lutful Hassan [2]

[1]Department of Computer Engineering, University of Kalyani, Kalyani, Nadia-741235, West Bengal, India

[2]A.K.C. School of I.T, University of Calcutta, Kolkata, West Bengal, India

ABSTRACT

In this paper a novel technique has been proposed for intrusion detection in MANET, where agents are fired from a node for each node randomly and detect the defective nodes. Detection is based on triangular encryption technique (TE)[9,10], and AODV[1,2,3,8] is taken as routing protocol. The scheme is an 'Agent' based intrusion detection system. This technique is applied on two types of defective nodes namely packet sinking and black hole attack. For simulation purpose we have taken NS2 (2.33) and three type of parameters are considered. These are number of nodes, percentage of node mobility and type of defective nodes. For analysis purpose 20, 30, 30, 40, 50 and 60 nodes are taken with variability. Percentage of defectiveness as 10%, 20%, 30% and 40%.Packet sink and black hole attack are considered as defectiveness of nodes. We have considered generated packets, forward packets, average delay and drop packets as comparisons and performance analysis parameters.

KEYWORDS

Agent Based Intrusion Detection System (AIDS), MANET, NS2, AODV, Mobile Agent, Black hole Attack

1. INTRODUCTION

As MANET is infrastructure less and also has the ability of node mobility and it is distributed in nature. Every node act as router So security is the main challenge in MANET [1][2][3] . MANET routing protocols are basically three types, they are Proactive or Table driven Reactive or On Demand, and hybrid routing protocol, which is combination of proactive and reactive. AODV[1,2,3,8,12] is on demand routing protocol. Which find the route on the basis of on demand. In AODV[1,2,3,8,12] a node want to send a packet it broadcast a route request message (RERQ). With the help of RERQ message AODV [1, 2, 3, 8,12] routing protocol create the route. In this routing protocol when nodes are moving the same process apply to find new route.

As the security is the main challenge of MANET, as MANET is dynamic in nature. There are basically two types of attacks in MANET. They are passive attack and active attack. A Passive attack does not disrupt the operation of the network. It just snoop the data without any alert from the network and confidentiality of the data has been lost. It is very hard to detect the passive attack in the network. The active attacks destroy the data and disrupt the operation of the network. Black hole attack is the example of active attack. Attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets wants to intercept. An attacker listen the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the

DOI : 10.5121/ijnsa.2013.5515

malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can drop the packets between them to perform a denial-of-service attack. Many researchers have proposed and implemented various 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 [15] 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.

Based on the sources of the audit information used by each IDS,[15] the IDSs may be classified into

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

Distributed IDSs. In this distributed IDS, 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 network based 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 destination.

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. Two type of defectiveness are considered here one is simple packet sink in any node (malicious node), another is black hole.

Black hole [11, 14, 16] attack is an active type of attack in MANET. This type of attack the attacker selectively drop RREQ/RREP message. In this type of attack malicious node waits for neighbouring nodes to send RREQ messages. When RERQ message is send to neighbour without checking its routing table then the malicious node sends immediately a false RERP message for route destination. So sending node considered that route has been discovered and it will ignore other RERP message. And victim node sends the data towards the malicious node. And black hole attack occurred in the network.

Section 2 of the paper deals with the proposed detection technique. Simulation environment has been presented in section 3. Section 4 deals with simulations. In section 5 results and comparison of performance are described. Conclusion is drawn in section 6 and conclusion is given at end.

2. PROPOSED TECHNIQUE

In proposed method AODV [1, 2, 3, and 8] is taken as routing protocol. A mobile agent named 'IDECT' fired from a monitor 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 . 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. The agent 'Idect 'randomly triggered its process of detection in randomly selected node computes 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 and also the detection status is shown in the system terminal. 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 XNOR ed, 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… 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… $s^{j+1}_{n-(j+2)}$ 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… $s^j_{n-(j-1)}$. 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… s^0_{n-2} s^0_{n-1} is shown in figure 1.

S= s^0_0 s01 s^0_2 s^0_3 s^0_4 s^0_5 ..... s^0_{n-2} s^0_{n-1}

S^1 = s^1_0 s11 s^1_2 s^1_3 s^1_4..... s^1_{n-2}

S^2= s^2_0 s21 s^2_2 s^2_3 … s^2_{n-3}

s^{n-2} = s^{n-2}_0 s^{n-2}_1

S^{n-1}= s^{n-1}_0

Figure 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. After that 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 non malicious otherwise it designate the node as malicious and mark the node accordingly before dropping of the Idect. The graphical view of an ideal 'Idect' is given in figure 2.

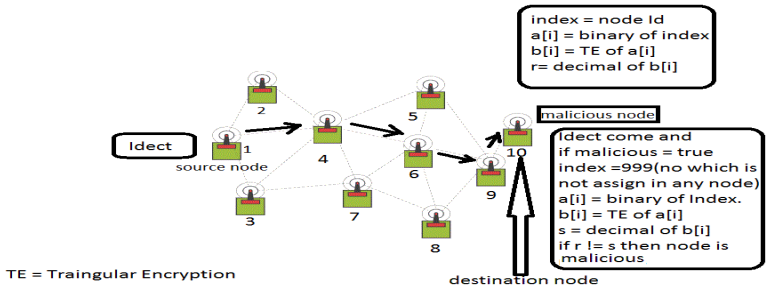

Figure 2 Graphical view of IDS technique

3. Simulation Environment

Network Simulator 2 (NS2.33) [6][7] is taken as a tool for simulation purpose. The Network Simulator 2 is widely used tool in network research and network industry. It is discrete event simulation, and capable of simulating various types of networks. NS2 [6, 7] consists of two languages, C++ and Otcl. In the back end C++, which defines the internal mechanism of the simulation object, and the front end 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.

3.1. Implementation of this Technique in NS2.

For the implementation of this technique an agent IDECT(protocol) is created in NS2 and this 'Idect' is merge with NS2[6,7] package . AODV routing protocol is taken as a routing protocol. Simple packet sinking technique is implemented adding some code in AODV.CC file. A specific node is configured as malicious in the scripting file (.tcl) file then the malicious behaviour of the node will be activated. As the nature of malicious is defined in aodv.cc file then it will drop the packet accordingly. Now this Technique is applied against to the sink of the packet in aodv.cc file. When the Idect agent come and going authenticate .if the destination node is malicious then Idect will be going to drop. Before dropping Idect will indicate that the node is malicious. In the other hand black hole attack is implemented in AODV protocol. When Idect come to the black hole node and try to authenticate the node with our proposed technique, and authentication will be failure and 'Idect' going to drop because node is black hole node. And before dropping Idect, it will also indicate that the node is black hole node. This technique is applied in blackholeaodv.cc file.

4. Simulations Parameters

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 and 60)
ii. Types of malicious : simple packet sink and black hole attack
iii. Percentage of malicious node (10%, 20%, 30% and 40%)

Snapshot of simulation output is given in figure 3 and 3.1 where outputs of various parameters are shown in details

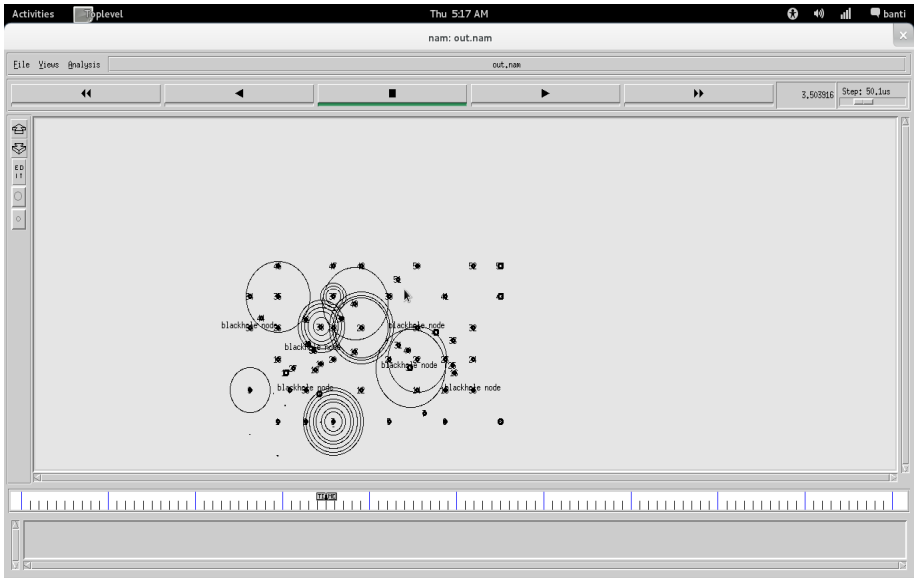

Figure 3. Snapshot of simulation in network animator (NAM)

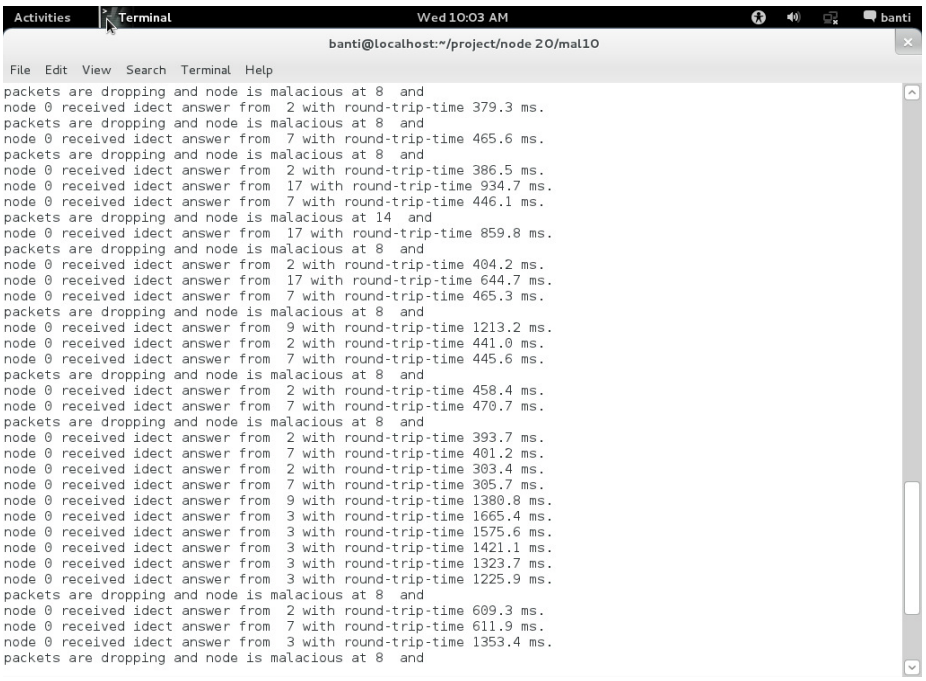

Figure 3.1. Snapshot of simulation in terminal

5. Performance analysis and Comparison

On applying this technique effect of performance in the network is described below.
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, two types malicious and percentage of malicious node. Numbers of nodes are taken 20, 30, 40, 50 and 60. The malicious types are considered simple packet sink and black hole attack and percentage of node malicious is taken as 10%, 20%, 30%, and 40%.

A. Generated packet

Comparison of the Idect packet generation is given bellow

a. *When 20 nodes are taken*: the comparison of generation packets given in the fig 4. In this figure it is seen that packet (Idect) generation is high when black hole attack occurred than simple packet sink attack occur, except when % of malicious is 10%.

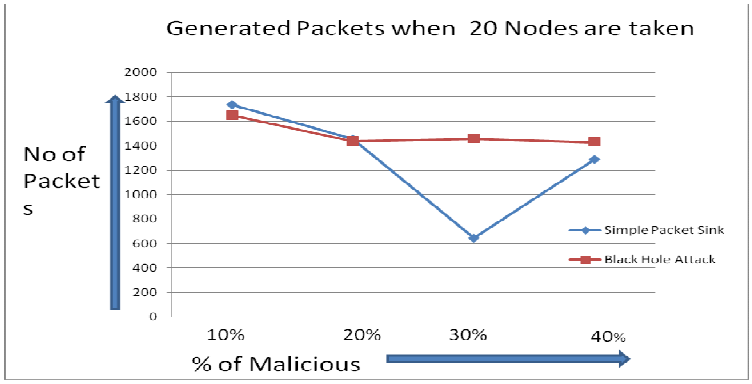

Figure 4. Generation of packets when nodes are 20 in the network

b. *When 30 nodes taken*: the comparison of generation packets is given in the fig 5. In this figure it is seen that packet (Idect) generation is always high when packet sink attack occur than black hole attack occur.

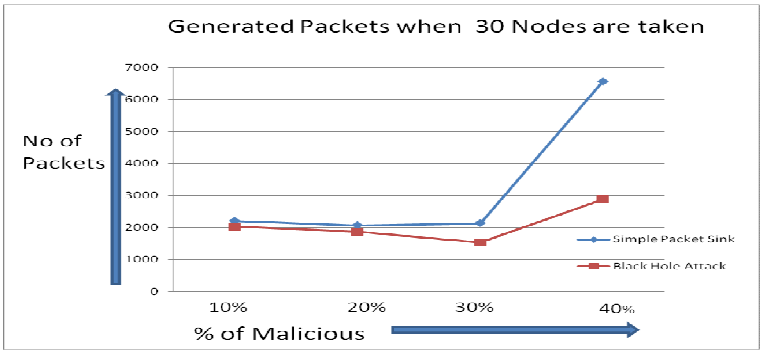

Figure 5. Fig4. Generation of packets when nodes are 30 in the network

c. *When 40 nodes taken*: the comparison of generated packets is given in the fig 6. In this figure it is seen that packet (Idect) generation is always high in packet sink attack than black hole attack.

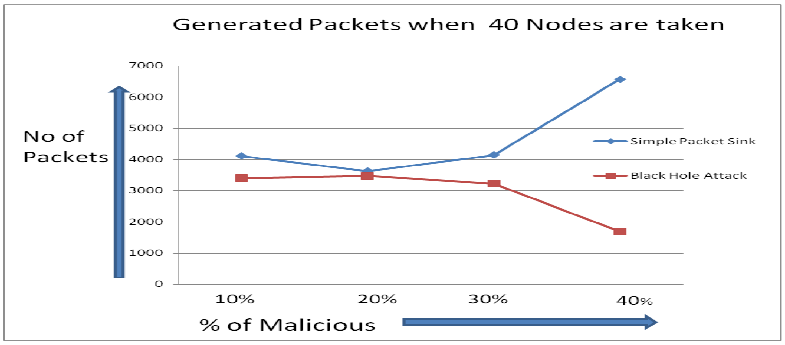

Figure 6. Generation of packets when nodes are 40 in the network

d. *When 50 nodes taken*: the comparison of generated packets is given in the fig 7. In this figure it is seen that packet (Idect) generation is higher in simple packet sink nature than black hole attack.

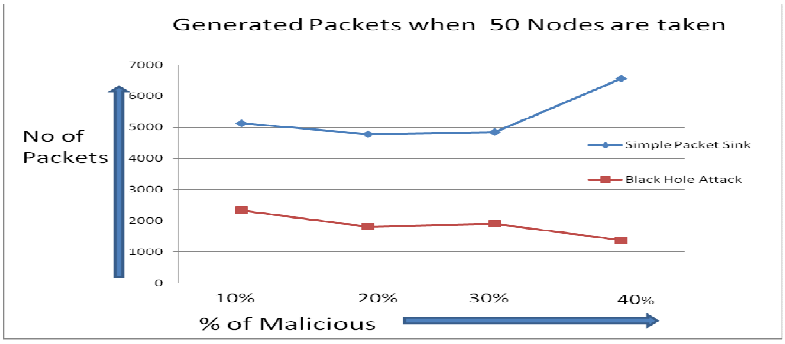

Figure 7. Generation of packets when nodes are 50 in the network

e. *When 60 nodes taken*: the comparison of generated packets is given in the fig 8. In this figure it is seen that packet (Idect) generation is of simple packet sinking behavior is higher than black hole attack like above figures.

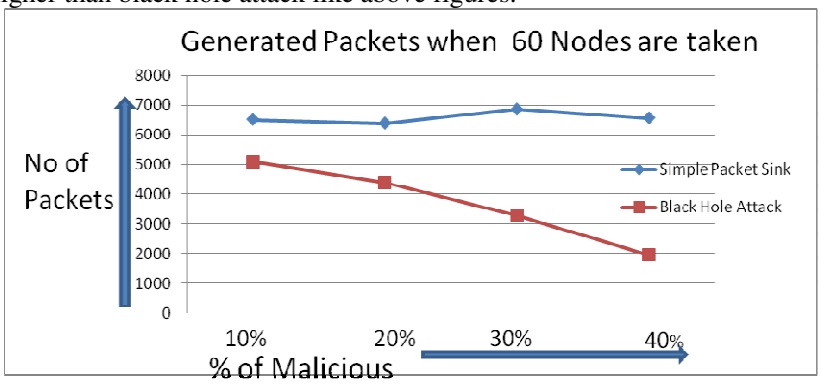

Figure 8. Generation of packets when nodes are 60 in the network

From the above figure 4,5,6,7 and 8 it is seen that number of packet generation is less in the where black hole attack occur. Only figure 4 shows that when node number is 20 at that time result of packet generation is mixed.

B. Forward Packets:
Comparison of forward packets are given bellow

a. *When 20 nodes taken*: the comparison of forwarded packets is given in the fig 9. In this figure it is seen that packet forward of black hole attack is higher than simple packet sink behavior of the nodes except when %malicious is 10%.

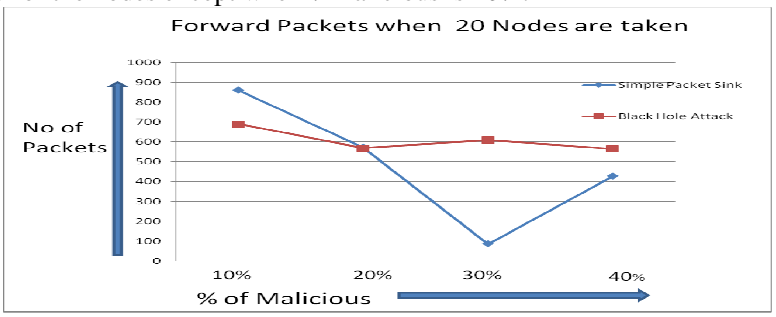

Figure 9. Forward packets when nodes are 20

b. *When 30 nodes taken*: the comparison of forwarded packets is given in the fig 10. In this figure it is seen that packet forward is higher in black hole attack than simple packet sink behavior.

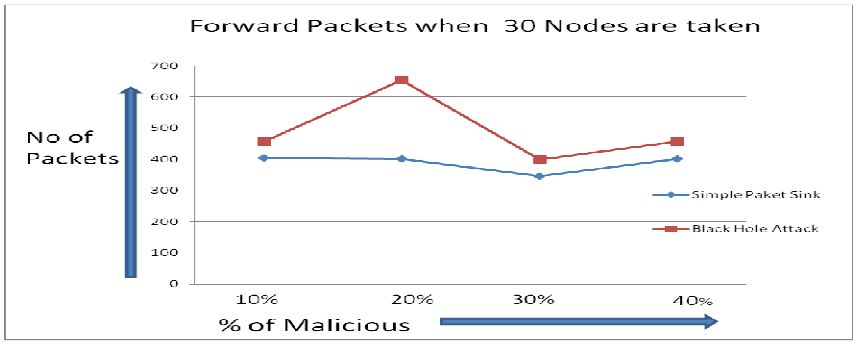

Figure 10. Forward packets when nodes are 30

c. *When 40 nodes taken*: the comparison of forwarded packets is given in the fig 11. In this figure it is seen that packet forward of black hole attack is higher than simple packet sink behavior of the nodes except when %malicious is 10%.

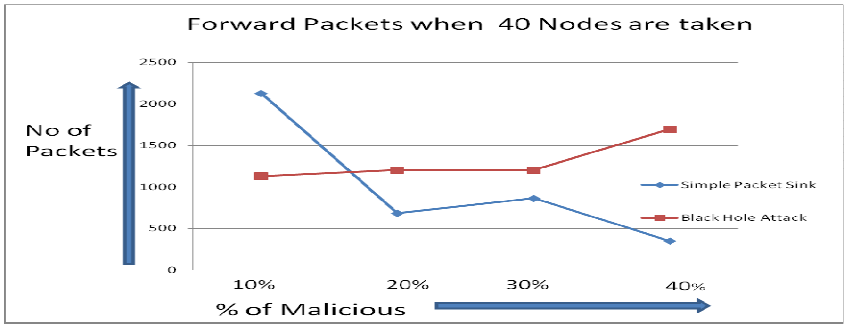

Figure 11. Forward packets when nodes are 40

d. *When 50 nodes taken*: the comparison of forwarded packets is given in the fig 12. In this figure it is seen that packet forward of black hole attack is higher than simple packet sink behavior of the nodes except when %malicious is 10% and 20%.

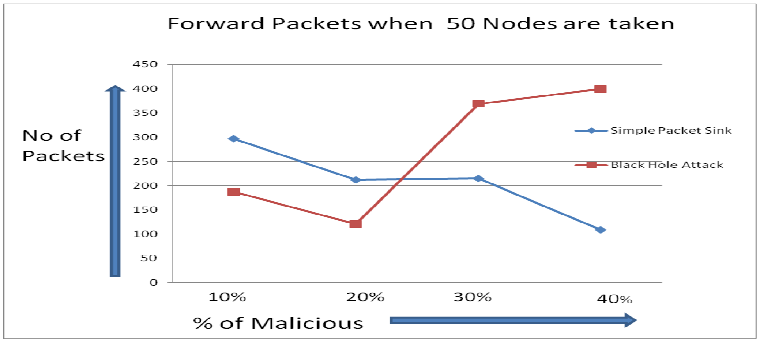

Figure 12. Forward packets when nodes are 50

e. *When 60 nodes taken*: the comparison of forwarded packets is given in the fig 13. In this figure it is seen that packet forward of black hole attack is always higher than simple

packet sink behavior. Difference between both is increased with increase of % of node malicious.

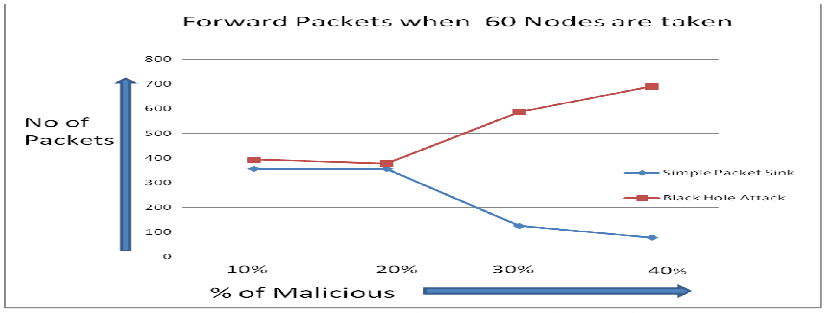

Figure 13. Forward packets when nodes are 60

From the above figure 9,10,11,12 and 13 it is seen that generally number of forward packet is more in those network where black hole attack occurs. Sometime this is violated. It may cause of another parameters.

C. Average Delay

Comparison of Average Delay are given bellow

a. *When 20 nodes taken*: the comparison of average delay is given in the fig 14. In this figure it is seen that average delay of data transmission in the network traffic is very low when black hole attack occur than simple packet sinking behavior.

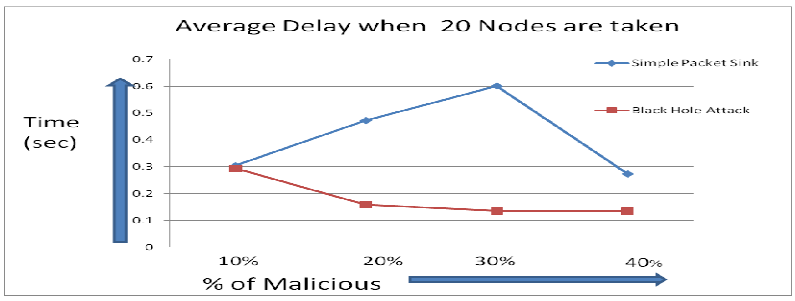

Figure 14. Average Delay when nodes are 20

b. *When 30 nodes taken*: the comparison of average delay is given in the fig 15. In this figure it is seen that average delay of data transmission in the network traffic is higher when black hole attack occur than simple packet sinking behavior except 20% node malicious. At 20% node malicious in both cases the average delay is about equal.

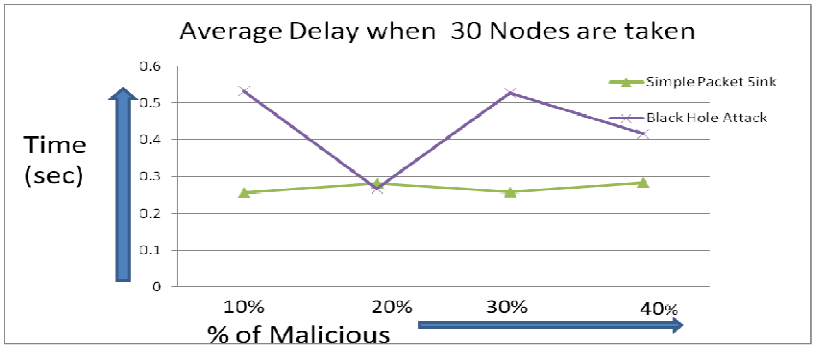

Figure 15. Average Delay when nodes are 30

c. *When 40 nodes taken*: the comparison of average delay is given in the fig 16. In this figure it is seen that average delay of data transmission in the network is lower when black hole attack occur than simple packet sinking behavior. But when % of malicious is 40% the average delay increased rapidly than simple packet sinking behavior.

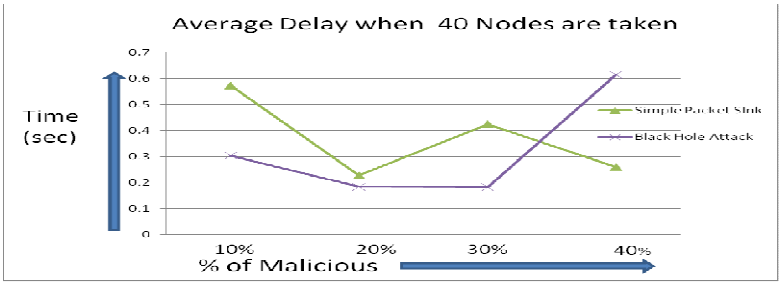

Figure 16. Average Delay when nodes are 40

d. *When 50 nodes taken*: the comparison of average delay is given in the fig 17. In this figure it is seen that average delay of data transmission in the network more or less equal .when % of malicious is 10% , average delay of black hole attack is a little higher

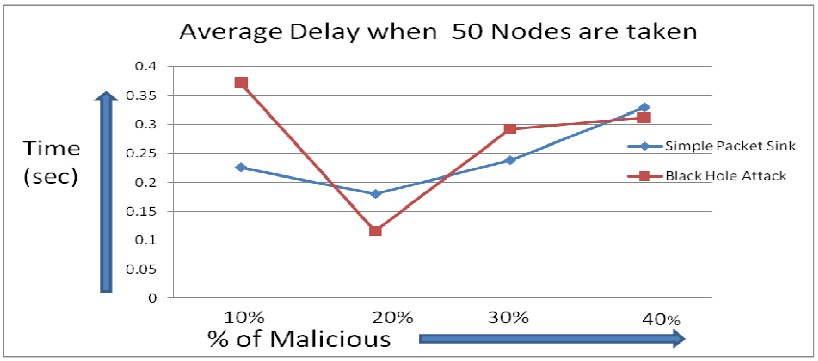

Figure 17. Average Delay when nodes are 50

e. *When 60 nodes taken*: when 60 nodes are taken the average delay of black hole attack is very high than simple packet sinking behavior in the network. Fig. 18 shows the comparison of average delay.

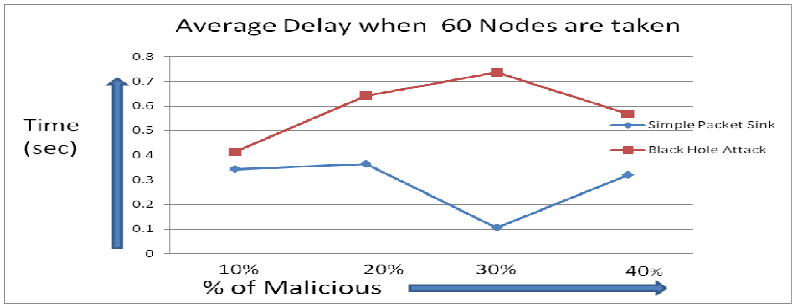

Figure 18. Average Delay when nodes are 60

From the figure 14 and 16 when node number is 20 and 40 the average delay is less in the networks where black hole attack occurs. From the figure 15 and 18 it is seen that when node number is 30 and 60 where black hole attacks occur the average delay is more. From the figure 17 where node number is 50 gives the mixed feedback.

D. Number of drop packets

Comparison of number of drop packet are given below

a. *When 20 nodes taken:* comparison of drop packets are shown in the fig. 19 when 20 nodes are taken. Number of packet drop of simple packet sink behavior is higher than black hole attack.

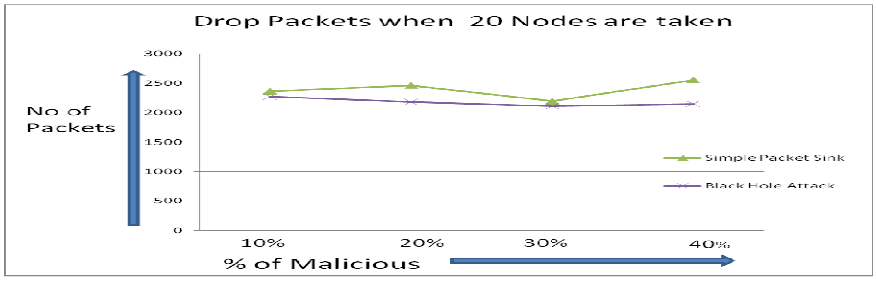

Figure 19. Number of drop packets when nodes are 20

b. *When 30 nodes taken:* comparison of drop packets are shown in the fig. 20 when 30 nodes are taken. Drop packet of black hole attack is less than simple packet sink behavior in the network.

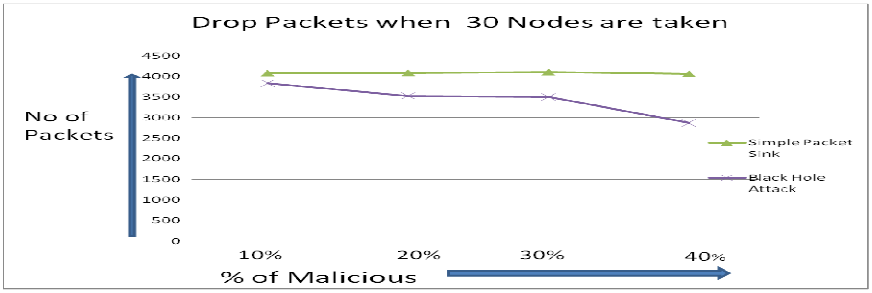

Figure 20. Number of drop packets when nodes are 30

c. *When 40 nodes taken:* comparison of drop packets are shown in the fig. 21 when 40 nodes are taken. Drop packets of black hole attack is very less than simple packet sink behavior of the network

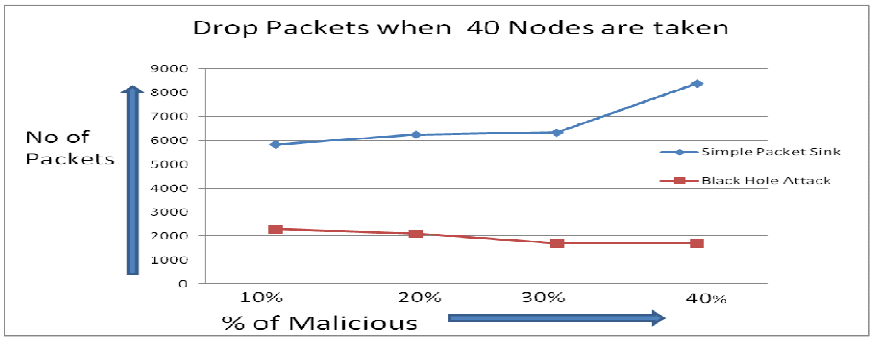

Figure 21. Number of drop packets when nodes are 40

d. *When 50 nodes taken:* comparison of drop packets are shown in the fig. 22 when 50 nodes are taken. In this figure it is seen that drop packet of black hole attack is also very less than simple packet sink behavior of the nodes.

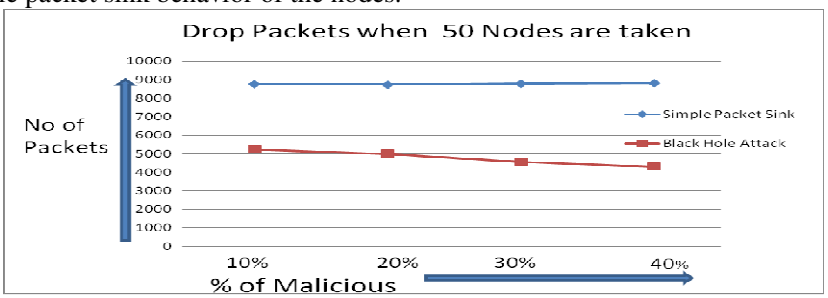

Figure 22. Number of drop packets when nodes are 50

e. *When 60 nodes taken:* comparison of drop packets are shown in the fig. 23 when 60 nodes are taken. This figure also represented that black hole attack has less packet drop than other one.

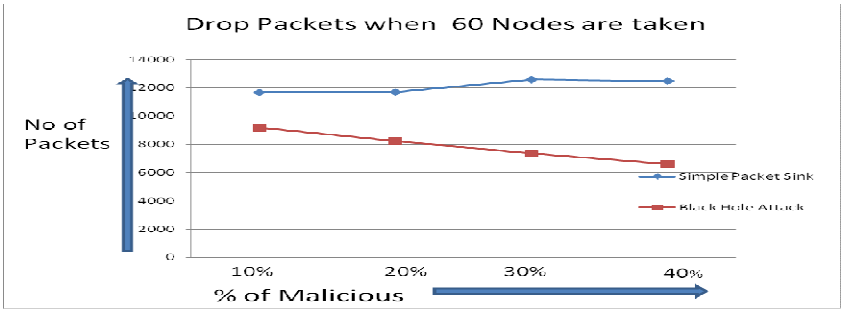

Figure 22. Number of drop packets when nodes are 50

From the figure 19,20,21,22 it is seen that number of drop packet are less where black hole attack occur than the network where simple packet sink occur.

3. CONCLUSIONS

In this paper a novel technique is proposed and applied to detect intrusion in MANET using mobile Agent ('Idect'). This novel technique is applied on two types of intrusion nodes, they are simple packet sink nodes and another is black hole node. This technique successfully detects the nodes with both type of defectiveness in the MANET. Comparisons 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).and maximum 40% nodes are malicious .If any network consist about 40% defective nodes then it can behave abonormally. 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 propose 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.

For future work this simple technique can be applied in the other types of attacks like gray hole attack , warm hole attack etc as well as this technique can be applied in other routing protocols.

ACKNOWLEDGEMENTS

The authors express deep sense of gratuity towards the Dept of CSE University of Kalyani where the computational resources are used for the work and the PURSE scheme of DST, Govt. of India.

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.

[16] Usha, Bose "Understanding Black Hole Attack in Manet" European Journal of Scientific Research, ISSN 1450-216X Vol.83 No.3 (2012), pp.383-396

AUTHORS

Jyotsna Kumar Mandal, M. Tech.(Computer Science, University of Calcutta),Ph.D.(Engg., Jadavpur University) in the field of Data Compression and Error Correction Techniques, Professor in Computer Science and Engineering, University of Kalyani, India. Life Member of Computer Societ y of India since 1992 and life member of cryptology Research Society of India. Ex-Dean Faculty of Engineering, Teachnology & Management, working in the field of Network Security, Steganography, Remote Sensing & GIS Application, Image Processing. 26 years of teaching and research experiences. Nine Scholars awarded Ph.D. and eight are pursuing. Total number of publications is two hundred seventy seven in addition of publication of five books from LAP Lambert, Germany.