Intrusion Detection System using Node Analysis in Wireless Networks

Sathiyaprabha R.
ME SE
PSG College of Technology
Coimbatore

T. Anusha
Assistant Professor
PSG College of Technology
Coimbatore

ABSTRACT
The threat of cyber intrusion is progressively high and harmful. Intrusion Detection Systems (IDS) provides the ability to identify security breaches in a system. A security breach will be taking any action based on the owner of the system believes unauthorized. Attacks in Wireless Networks (WNs) aim in limiting or even eliminating the ability of the network to perform its expected function. WNs are networks with limited resources and often deployed in uncontrollable environments that an intruder can easily access. WN attacks target specific network layer's vulnerabilities but normally affect other layers as well. Network layer should be monitored and evaluated in order to detect possible malicious intervention. In this research, a general methodology of an anomaly-based Intrusion Detection System is proposed and evaluated the proposed system using routing layer attacks in Ad-hoc Distance Vector Routing (AODV) protocol and IDS is able to detect malicious activity and our solution delivered the packets to the receiver in a new route without discarding.

General Terms
Security, Black hole, Gray hole, Selective Dropping

Keywords
WN, IDS, AODV.

1. INTRODUCTION
Security is becoming precarious issue as the Internet applications are growing. At present the security technologies are focusing on firewall, encryption and access control. But these technologies cannot assure a security without any imperfections or defects. The system security can be improved by Intrusion detection. The IDS that is able to classify intrusions in real time with accurate results is important. The patterns of user activities and audit records can be examined and the intrusions can be detected.

IDS is used for monitoring the network and protecting the network from the invader. Nowadays, hackers are using different types of attacks to get the valuable information. Hence security is much needed for the users to secure their system from the invaders. Network Intrusion Detection System(NIDS) are placed at a strategic point within the network to monitor traffic to and from all devices on the network. NIDS performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed and attacker node is displayed. Thus, IDS are becoming essential for network users. The AODV protocol, starts the route formation when the source node has some transmission data. The AODV maintains and uses the same routing information as long as the transmission lasts and the route remains stable. It makes use of broadcasted RREQ messages to form paths and, upon receiving these messages, the intermediate nodes forward them further and responds back on behalf of the destination. The RREP message is sent as a unicast message to the source node using information gathered by intermediate nodes. This process also helps the nodes to learn about the forward and reverse path between the communicating nodes. Thus, AODV protocol helps in reducing the control traffic in the network, which, in turn, gives it an edge over proactive routing protocols used by Mobile Ad Hoc Network (MANET).

Network Simulator-2 (NS-2) is an open source, event driven system that is developed using C++ and Tool Command Language(TCL) language. In NS2, researchers can easily add new components and functions to the system to serve their own purposes. The latest version of NS-2 supports most of the standard protocols. In order to analyze security features for the network, needs to add security module into NS-2.

2. RELATED WORK
Christiana Ioannou, Vasos Vassiliou et al [1] proposed a Wireless Sensor Networks (WSNs) with black hole and gray hole attacks. The WSN aim in limiting or even eliminating the ability of the network to perform its expected function. The Binary Logistic Regression (BLR) statistical tool is used to classify local sensor malicious activity to either benign or malicious and evaluated the proposed system using routing layer attacks and showed that IDS is able to detect malicious activity within the range of 88%-100%.

Sydney Mambwe Kasongo et al [2] proposed a IDS where networks are coupled with a filter-based feature selection algorithm, which is then evaluated using the well-known data mining (NSLKDD) dataset and it is compared to the following existing machine learning methods: support vectors machines, decision tree, K- Nearest Neighbor, and Naive Bayes and the metric used is precision, which shows a less error rate.

Yihan Xiao et al [3] proposed a network intrusion detection model based on a convolutional neural network IDS. Redundant and irrelevant features in the network traffic data are first removed using different dimensionality reduction methods. Features of the dimensionality reduction data are automatically extracted using the CNN and more effective information for identifying intrusion is extracted by supervised learning. To reduce the computational cost, the original traffic vector format is converted into an image format and used a standard KDD-CUP99 dataset to evaluate the performance of the proposed CNN model. The experimental results indicate the Accuracy, False Alarm Rate (FAR) and timeliness of the CNN_IDS model are higher than those of RNN and DNN.

Aman deep Kaur, Prakash Rao Ragiri [4] proposed a Mobile Ad-hoc Network where gray hole attack targets the routing

protocol of the network and AODV is prone to gray hole attack due to lack of central control and security. The result of the AODV protocol is simulated in different scenarios, the impact of gray hole attack is observed and compared with a normal scenario.

3. PROPOSED WORK

This section explains the proposed system about identifying attacker nodes and to set a new path to send different packets to the destination node.

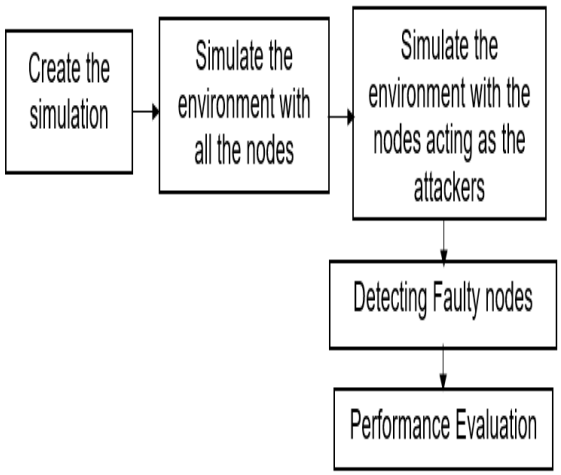

Fig 1: Block diagram of the proposed work

3.1 Simulation environment

Created a wireless network with a following configuration. Number of mobile nodes:25, number of packets:50, mac type:802.11, network interface type as wireless physical, antenna model as Omni- Antenna, energy model with initial energy:10, protocol: AODV. The simulation can be viewed in a network animator (NAM).

3.2 Simulate the environment with all the nodes

The NS2 simulator is used and designed, programmed the modules and implemented the various classes to work with existing NS2 modules. Several modifications were also carried out on existing NS2 modules to incorporate the various required node behaviors and the overall functionality of the proposed system. A single node is set initially as a receiver node and all other nodes acts as sender nodes. In the simulation the communication among the nodes can be viewed. The 12th node is made the receiver node, that receives packets from other nodes.

3.3 Simulate the environment with the nodes acting as the attackers

The attacks were given in the Ad-hoc protocol. The attacks were given in Ad-hoc distance vector protocol in a forward packet class. The packets that are sent to the receiver is disrupted. The attacks used here is,

3.3.1 Black Hole Attack

It is also a packet drop attack. Black hole attack is a type of denial-of-service(DOS) attack in which a router that is supposed to relay packets instead discards them. In the black hole attack the node 8 is made as a Black Hole attacker node. All the packets coming from the node 8 is dropped. So the packets that is coming from node 8 is not received by the receiver.

3.3.2 Gray Hole Attack

A gray hole attack is extension of black-hole attack used to bluff the source and monitoring system by partial forwarding. Generally Gray Hole attack stores the address of the packets that is coming the nodes and discards selective packets from the nodes. In the Gray hole attack the node 16 is made as a gray hole attacker node. All the third packets coming from the node 16 is dropped. So the packets that is coming from node 16 is not completely received by the receiver.

3.3.3 Selective Dropping Attack

Selective Dropping attack is also one of the security attacks. The Selective Dropping attack does not store any address of the packets its coming from. It basically discards the selective packets it is obtaining. In the Selective Dropping attack, the node 18 ismade as a Selective Dropping attacker node. All the fifth packets coming from the node 18 is dropped. So the packets that is coming from node 18 is not completely received by the receiver.

3.4 Node monitors

Node monitors(NM) are nodes that do not contain any packets. This acts as a promiscuous mode. A new function is created in the AODV protocol, which acts as a solution to our problem. It does not involve in sending and receiving the packets. It just transmits the packets and make a count on how many packets have been sent and received by each neighbouring node. Node monitors stores the data of the neighbouring nodes as how much packets its being receiving and sending to the other node. It identifies the attacker nodes by finding the difference between the sent and received packets of each neighbouring nodes. After one neighbouring node has sent the packet, node monitor makes a count on that and after two seconds it checks other neighbouring nodes receiving packet because sending packets takes some time during their transfer in the path. If the packets discarded is greater than two packets, it identifies the specific node as the attacker node and displays. The attacker node is identified and in the forward path it is noted, the path is dropped and a new shortest path is created by the network in the AODV protocol and the packets is being transferred without discarding.

3.5 Performance Evaluation

In order to analyze the efficiency and other important aspects of the proposed solution in the standard AODV protocol the performance evaluation is done. For the performance evaluation the parameters input is taken from the trace file. The trace file is the one that runs at the backend when a simulation starts. Based on the simulation results, the parameters that are compared are:

3.5.1 Throughput

Throughput is the number of successfully received packets in a unit time. Average Throughput is the number of data bits delivered at the destination node in unit time.

$$\mathrm{T} = \frac{1}{n}\sum_{A=0}^{n}\frac{(N * 1024 * 8)}{Transmission\ Time}$$

Where:

A: application ID

N: total number of packets delivered

n: total applications

3.5.2 Delay

Delay is the difference between the time at which the sender generated the packet and the time at which receiver received the packet. Average End-to-End Delay is the difference in terms of delivery time of the first data packet at destination node to the time it was transmitted by the source node.

$$E = \frac{1}{n}\sum_{A=0}^{n}(tr - ts)$$

Where:

tr: Time of first received packet at destination.

ts: Time of first received packet at source.

4. RESULTS AND DISCUSSION

This section presents the experimental result in three cases like normal case, during attack and after finding a solution to overcome attacks.

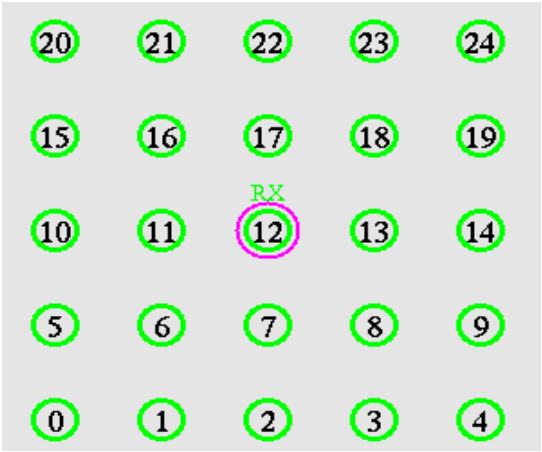

Fig 2: An environmental setup

An environmental setup is made and can be viewed in NAM. Fig 2. RX is 12th node acts as the receiver node. Where the other nodes send packets to the 12th node.

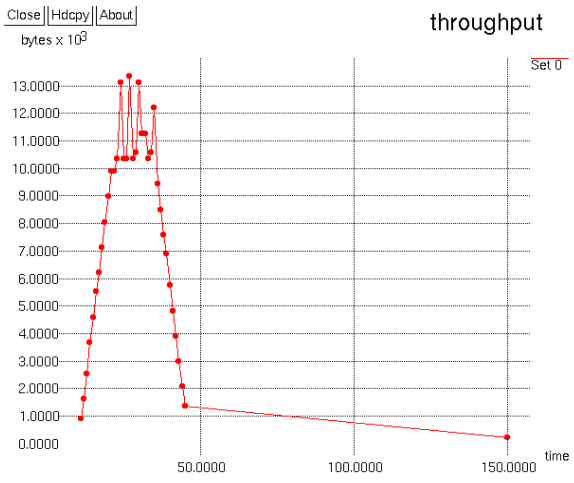

Fig 3: Throughput graph before attack

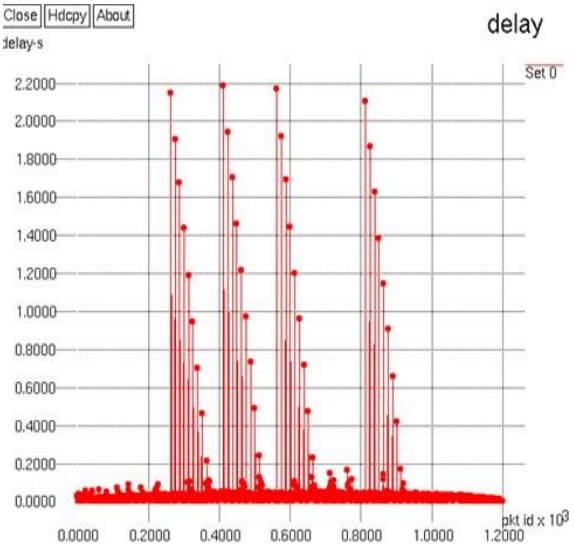

Fig 4: Delay graph before attack

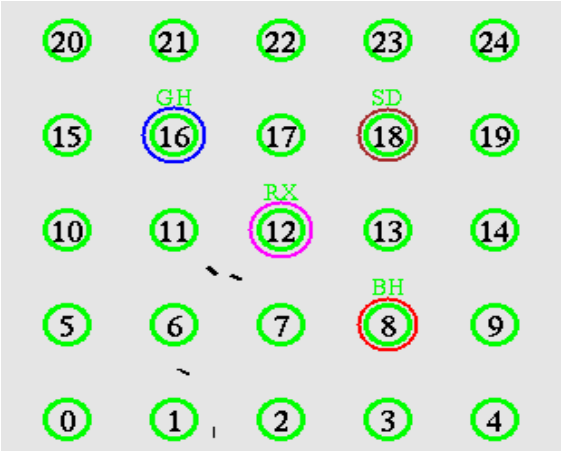

Fig 5: Attacker nodes

Fig 5 The attacker node is introduced, where 8th node is a black hole attacker node, 12th node is receiver node, 16th node is gray hole attacker node, 18th node is selective dropping attacker node.

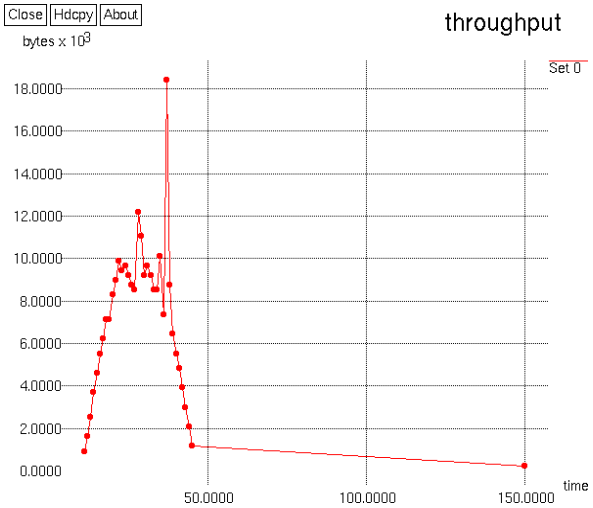

Fig 6: Throughput graph after attack

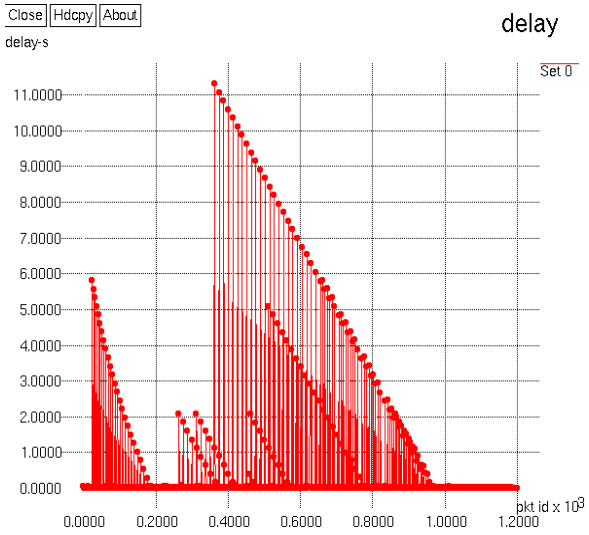

Fig 7: Delay graph after attack

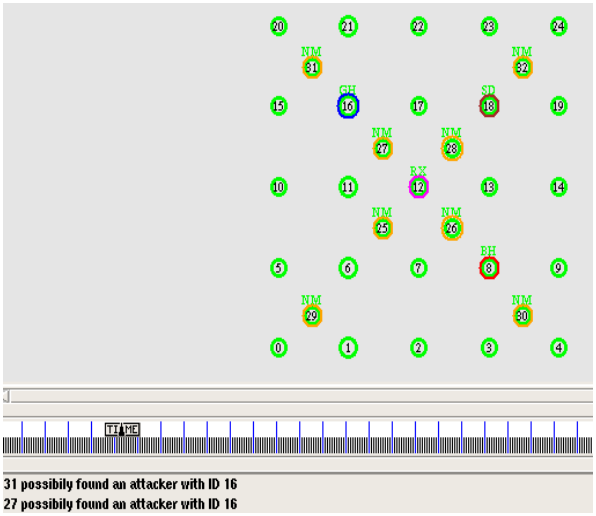

Fig 8: NAM console with node monitors

Fig 8 NM represents the node monitor nodes such as 25,26,27,28,29,30,31,32 nodes. Which monitors the sent and received packets and identifies the attacker node 16.

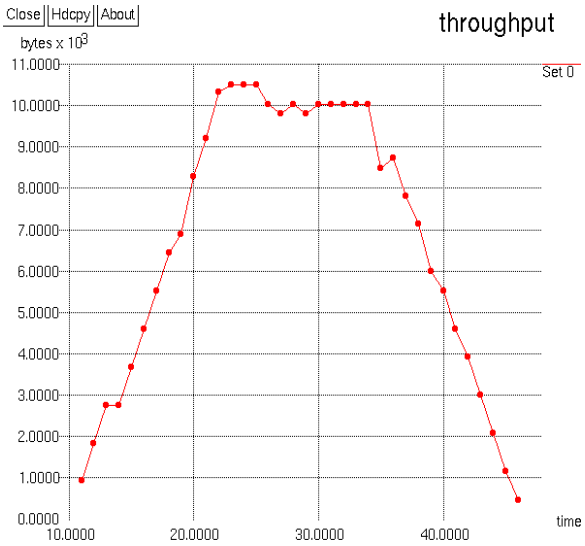

Fig 9: Throughput graph after finding attacker node

Fig 9 shows the increase in the throughput graph compared to the previous one.

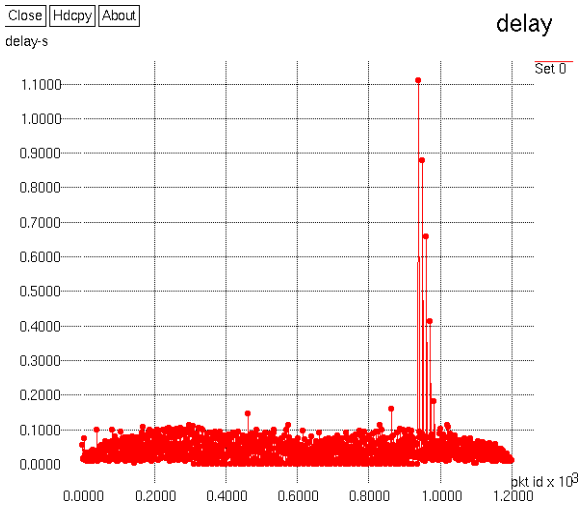

Fig 10: Delay graph after finding attacker node

5. CONCLUSION

The proposed methodology is an anomaly-based Intrusion Detection System (IDS). The study concludes that AODV and modified AODV is a useful routing protocol for establishment of a proper network. The complete work observes black hole, gray hole, selective dropping attacks as crucial threat and proposed a solution to overcome the problem of packet discard. The experimental results show the network simulation about how the communication happens among the nodes by sending and receiving the packets. The results prove that the attacks have been introduced and it has been detected by using a best possible solution. The future enhancement includes a study of many attacks and to evaluate the model with more attacks and implement the detection model with more nodes. It is also observed that, hostile environment may harm its performance in unbelievable manner so the vulnerabilities points should be identified and attacks should be prevented.

6. REFERENCES

[1] C. Ioannou, V. Vassiliou and C. Sergiou, "An Intrusion Detection System for Wireless Sensor Networks," 2017 24th International Conference on Telecommunications (ICT), Limassol, 2017, pp. 1-5, doi: 10.1109/ICT.2017.7998271.

[2] S. M. Kasongo and Y. Sun, "A Deep Learning Method With Filter Based Feature Engineering for Wireless Intrusion Detection System," in IEEE Access, vol. 7, pp. 38597-38607, 2019.

[3] Y. Xiao, C. Xing, T. Zhang and Z. Zhao, "An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks," in IEEE Access, vol. 7, pp. 42210-42219, 2019.

[4] Aman deep Kaur, Prakash Rao Ragiri, "Study of various Attacks and Impact of Gray hole attack over Ad- Hoc On demand (AODV) Routing Protocol in MANETS", International Journal of Engineering Research & Technology (IJERT), IJERT ISSN: 2278-0181, IJERTV3IS050721, www.ijert.org, Vol. 3 Issue 5, May – 2014.

[5] W. Zhu, M. Deng and Q. Zhou, "An intrusion detection algorithm for wireless networks based on ASDL," in

IEEE/CAA Journal of Automatica Sinica, vol. 5, no. 1, pp. 92-107, Jan. 2018.

[6] P. Tao, Z. Sun and Z. Sun, "An Improved Intrusion Detection Algorithm Based on GA and SVM," in IEEE Access, vol. 6, pp. 13624-13631, 2018.

[7] Yu, Dunyi,"Research on Anomaly Intrusion Detection Technology in Wireless Network," 2018 International Conference on Virtual Reality and Intelligent Systems (ICVRIS), Changsha, 2018, pp. 540-543.

[8] H. Alipour, Y. B. Al-Nashif, P. Satam and S. Hariri, "Wireless Anomaly Detection Based on IEEE 802.11 Behavior Analysis," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 10, pp. 2158-2170, Oct. 2015.

[9] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," WiMob'2005), IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005., Montreal, Que., 2005, pp.

[10] A. Yang, Y. Zhuansun, C. Liu, J. Li and C. Zhang, "Design of Intrusion Detection System for Internet of Things Based on Improved BP Neural Network," in IEEE Access, vol. 7, pp. 106043- 106052, 2019.

[11] H. Yang and F. Wang, "Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network," in IEEE Access, vol. 7, pp. 64366-64374, 2019.

[12] J. Abo Nada and M. Rasmi Al-Mosa, "A Proposed Wireless Intrusion Detection Prevention and Attack System," 2018 International Arab Conference on Information Technology (ACIT), Werdanye, Lebanon, 2018,pp.1-5.

[13] Rupali Sharma ,"Gray-hole Attack in Mobile Ad- hoc Networks : A Survey", International Journal of Computer Science and Information Technologies, Vol. 7 (3), 2016.

[14] Marepalli Radha, M. Nagabhushana Rao, "Gray Hole Attack Detection Prevention and Elimination using Sdpegh in Manet", International Journal of Engineering and Advanced Technology(IJEAT), ISSN: 2249 – 8958, Volume-8 Issue-3, February 2019.

[15] Anubha Goyal, "Selective Packet Drop Attack in MANET-A Review", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May-2014.

[16] P. Tao, Z. Sun and Z. Sun, "An Improved Intrusion Detection Algorithm Based on GA and SVM," in IEEE Access, vol. 6, pp. 13624-13631, 2018.