Intrusion Detection In Wsn Using Modified AODV Algorithm

S.Rajesh[1*], M.Sangeetha[2]
{rajeshsports@gmail.com[1], sang_gok@yahoo.com [2]}

Research Scholar, Department of Electronics and Communication Engineering, Bharath Institute of Higher Education and Research Chennai, India.[1]
Professor & Head, Department of Electronics and Communication Engineering, Bharath Institute of Higher Education and Research, Chennai, India.[2]

Abstract. Wireless sensor network plays a major role in recent scientific developments for transmission of information. It comprises of many sensor nodes which are connected virtually to transmit and receive data. But security is the main challenge experienced in the WSN to have a proper data transmission. Hence detection and separation of the attacks created in the sensor network is necessary. In this paper, a scheme for intrusion detection in wireless sensor network is introduced. It is done by using a modified AdhocOn Demand Distance Vector (AODV) algorithm as a routing protocol. Here NS-2 is used for implementing and simulating the proposed protocol and its performance is evaluated and analysed considering various network parameters.

Keywords: Wireless Sensor Network, Intrusion Detection, AODV, Routing, NS -2m.

1 Introduction

Wireless Sensor Networks are employed in various applications like object tracking, process monitoring, home health tracking, traffic monitoring, industrial automation etc., It is a framework of several sensor nodes with limited resources, little power and finite bandwidth. As the WSN are mostly constructed in unmonitored area it is highly prone to attacks from intruder which results in destruction of information. Hence Intrusion Detection System (IDS) is introduced as network security scheme to prevent or minimize loss of information. IDS are a set of tools to recognize, analyze and report malicious activity in the network for securing the data. The intrusions are of two kinds namely signature based detection and anomaly detection. In the first detection, the already executed attack patterns are predefined and the when same method of attack is replicated it will be detected and reported. The drawback of this type is new attacks can’t be discovered. In the second type of detection the normal behavior of the nodes are established and monitored for deviations. If any such abnormal behavior is detected it is categorized as intrusion. This often results in false negative rate.

Sensor Network Attacks

In any network secrecy and authentication has to be maintained. But to manipulate the genuineness of a network many types of attacks are created by the intruders. Some of the types are discussed below.

I3CAC 2021, June 07-08, Chennai, India

DOI 10.4108/eai.7-6-2021.2308629

Denial of Service (DoS) Attacks: This attack is created to crash the network with unusual traffic by flooding unwanted requests into the network. It absorbs the network resources and drains the energy.

Spoofing and Altering of Routing Information: Here the nodes are disguised by the attacker and rerouting of the traffic is done to create traffic.

Selective Forwarding: The intruder makes the vulnerable nodes to randomly drop some packets during transmission from source to destination. The forwarding of packets is decided by the attacker.

Sinkhole Attacks: In this attack the traffic in a particular region is diverted to a compromised node by faking the routing algorithm. This attack is used to initiate other attacks like spoofing or selective forwarding.

Wormholes: It is a brilliant idea where the malicious node entraps the messages between two different regions of network at high speed to make distant nodes look nearer.

The Sybil Attack: The corrupted node will act as many other nodes in the network by acquiring false identity. This is used to confuse and divert the routing protocol.

Black Hole Attack: In this attack the malicious node discards the packets instead of forwarding them. This is done by portraying itself as shortest path to the source by giving Route Reply (RREP) message immediately.

2. Literature Survey

Intrusion Detection plays a predominate role in Wireless Sensor Networks. In this paper, Amrita Goshal et al., 2017 [1] summarizes about various parameters involved in intrusion detection system in terms of the energy consumption. Here the basics of intrusion detection system such as its working model, the challenges faced to maintain high accuracy rate and lower energy value are discussed. Since WSN works with moderate power reserve, limited transmission bandwidth and low memory dimensions the designing of IDS to achieve efficient result becomes complex. Here the various requirements to design energy efficient IDS and the classification of IDS are outlined. Further the various approaches of IDS to protect WSN are discussed and the accomplishment of existing systems in terms of energy utilization is tabulated and studied. It also pointed out the parameters to be considered for upcoming development in this area.

Linlin Li et al., 2018 [2], proposed a model for intrusion detection formulated on Danger Theory for danger perception and to find intrusion with a help of multimode system. Here Projection Pursuit Algorithm is used for danger perception and to control the problem arises due to heavy traffic. It also uses Extreme Learning Machine algorithm to classify the danger and Beta distribution for calculating the trust among the nodes. This paper proves that the danger theory used here shows better performance in terms of energy usage and false negative and positive rate compared to SNS model. The simulations are conducted here on MATLAB platform using KDD CUP99 dataset.

Artificial immune system concept has been adapted in many intrusion detection systems and one among them is negative selection algorithms. Some features of this algorithm are not given much importance while applying in wireless sensor network which results in lower efficiency. Hence Ruirui Zhang et al., 2019 [3], has formulated an improved negative selection algorithm based on spatial division. The dispensation of self- set in real value space is initially evaluated by the algorithm and then divided into many sub spaces. The selves are allotted to these sub spaces and the NSA is applied to the sub space. The selves in the sub space with the detector only can be put up with the randomly created candidate detector and not all the sub spaces. The antigen detection process is fastened due to this operation. The efficiency of this proposed algorithm is verified both theoretically and experimentally which shows good results in all parameters required for a better intrusion detection system.

Kenneth RodolpheChabiBoni et al., 2020 [4] has proposed a novel innovation in providing security for WSN. Here the intrusion detection system introduced is a device incorporated with the features of sensors. The algorithms required for finding and separating the intruder or the authentic node is computed by this new IDS device. It refines all the data passes through the sensors by constructing a virtual compound around them. This process along with the implementation of Trust Table concept helps in isolation process by keeping record of all the sensors in the network to prove the genuineness of the sensors and also to avoid the breaking of the service. Further this isolation method is also enhanced by bringing in the concept of Feedback Signal to alert the other sensors in the network about the suspicious sensor to avoid further correspondence from the corrupted one. This IDS also involves in data transmission over sensors with other distributed IDS across wide geographical region to detect and eliminate threats.

Rabie .A et al., 2020 [5] has explained about the sinkhole attack in the wireless sensor network and has proposed two algorithms for detection and prevention of this attack. Multipath based Intrusion Detection System (MBIDS) algorithm and Threshold Based Intrusion Detection System (TBIDS) are the two algorithms discussed in this paper. The first algorithm is based on routing where the data message is accompanied by a control message and the second algorithm works by inspecting the threshold values of each cluster head. Further in this paper three recent algorithms namely S-LEACH, MS-LEACH and ABC are compared with these two algorithms and the results obtained shows better performance with the proposed algorithms.

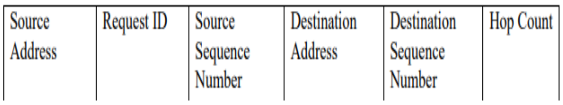
MdAlauddinRezvi et al., 2020 [6] describes about a data mining methodology which is used to examine the intrusion detection system of a wireless sensor network. Here the various Denial of Service attacks like Blackhole, Grayhole, TDMA and flooding are considered and different data mining techniques are applied to these datasets to analyze these attacks. The performance of algorithms like Logistic Regression, KNN, Naïve Bayes, support vector machine (SVM) and ANN algorithms in classifying and analysing the attacks are also evaluated here.

3. Proposed System

The aim of an attacker was to influence the user data in a network directly or by attacking the underlying routing algorithm. The routing protocol defines about how the communication between the nodes takes place and also way by which the data is transmitted. In the proposed system the intrusion done by the attacks like sink hole or black hole is detected and analyzed by a modified version of the Ad hoc On-Demand Distance Vector Routing (AODV) algorithm. This modified protocol also inhibits the features of the existing AODV.

The AODV falls under reactive protocol category. Here the routing is done only when a request arise and hence the name on – demand. When a source wants to send a packet to the destination a Route Request message (RREQ) is broadcasted in the network. The fields in the RREQ are as follows:

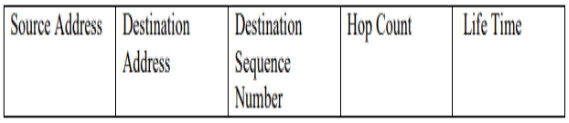
Table 1. Route Request field



Source Address	Request ID	Source Sequence Number	Destination Address	Destination Sequence Number	Hop Count

The node which receives this broadcast message checks its routing table for the known route to the destination. If it does not find any matching, it forwards the message to its neighbors. The neighboring nodes or the nodes in the relay in turn checks their routing table and if the destination is not found the cycle is repeated. When a node with the route for destination address or destination itself is found it sends a Route Reply (RREP) to the source which sent the request. The RREP framework is as below:

Table 2. Route Reply field



Source Address	Destination Address	Destination Sequence Number	Hop Count	Life Time

The RREQ message is recognized by the combo of its source address and request ID only. Every time when a new request message is sent by the source the request ID is increased. When a RREQ is received by a node it checks for the combo address of the request message and if it already exists then the new request sent will be discarded. If a node does not find a route for the destination address the Hop Count of the RREQ will be incremented and rebroadcasted to the neighbor nodes. The RREP message will be sent to the source node only if the sequence number of the node with the desired route is equal or greater to the RREQ.

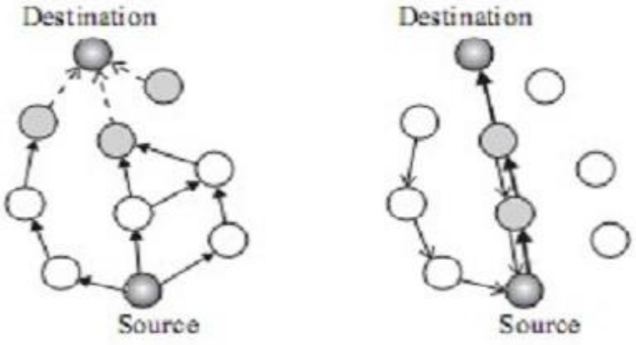


Fig 1. Discovery of route using modified AODV

4. Results And Discussions

NS 2 Simulator is used to analyze the performance of the modified AODV algorithm in the process of detection of intruders. The performance is measured based on the following metrics;

Average End to End Delay: The network delay is the time taken for the transmission of the packet from the source to the destination. The lower the value the efficiency of the protocol is higher.

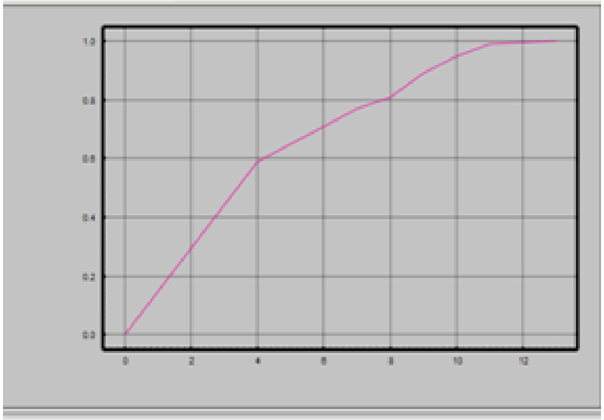


Fig 2. Average End to End Delay Graph

Throughput: It is the total packet size received per unit time and expressed as bytes/sec. This value has to higher to show a better performance.

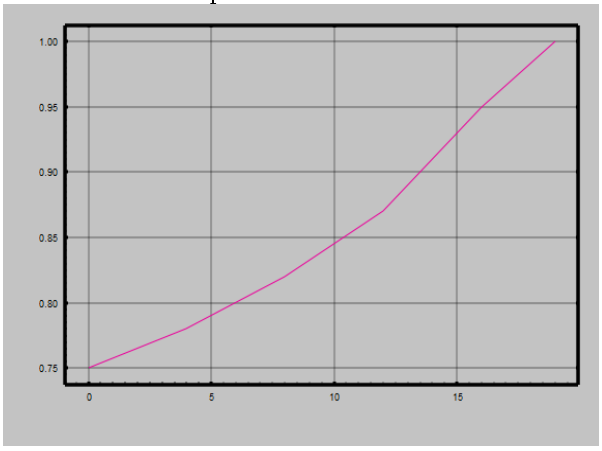


Fig3. Throughput Graph

Conclusion and future work

In this paper a modified Ad hoc On-Demand Distance Vector Routing is proposed for intrusion detection in wireless sensor network. The metrics such as end to end delay and throughput are evaluated by using the simulation results. The results show satisfactory performance with the modified routing protocol. In future the work can be established with higher number of nodes to improve the efficiency of complex network.

Conflicts of interest

- The authors should declare any conflicts of interest exist. If no conflict exists, the authors should state: the authors have no conflicts of interest to declare.

References

[1] Amrita Ghosal, SubirHalder (2017), “A survey on energy efficient intrusion detection in wireless sensor networks”, Journal of Ambient Intelligence and Smart Environments, Vol.9 pp. 239–261

[2] Linlin Li, Liangxu Sun, Gang Wang (2018), “An Intrusion Detection Model Based on Danger Theory for Wireless Sensor Networks”, International Journal of Online and Biomedical Engineering, Vol. 14, No. 9, eISSN: 2626-8493

[3] Ruirui Zhang, Xin Xiao (2019), “Intrusion Detection in Wireless Sensor Networks with an Improved NSA Based on Space Division” Journal of Sensors, https://doi.org/10.1155/2019/5451263

[4] Kenneth RodolpheChabiBoni, Lizhong Xu, Zhe Chen, Thelma Dede Baddoo (2020), “A Security Concept Based on Scaler Distribution of a Novel Intrusion Detection Device for Wireless Sensor Networks in a Smart Environment”, Sensors, doi:10.3390/s20174717

[5] Rabie A, Ramadan (2020), “Effiecient Intrusion Detection Algorithms for smart cities based Wireless Sensing Technologies”, Journal of Sensors and Actuator Networks, doi:10.3390/jsan9030039.

[6] MdAlauddinRezvi, SidratulMoontaha, Khadija Akter Trisha, ShamseTasnim Cynthia, Shamim Ripon (2020), “Data mining approach to analyzing intrusion detection of wireless sensor network”, Indonesian Journal of Electrical Engineering and Computer Science, Vol. 21, No. 1, pp. 516~523, ISSN: 2502-4752

[7] BinghuaHao, Dan Chang, Zengping Zhang, Hailong Ji (2019), “Performance Analysis of Routing for Wireless Sensor Network”, 3rd International Conference on Mechatronics Engineering and Information Technology, Advances in Computer Science Research, volume 87

[8] ItuSnigdh, DevashishGosain (2015), “Analysis of scalability for routing protocols in wireless sensornetworks”, Optik - International Journal for Light and Electron Optics, http://dx.doi.org/10.1016/j.ijleo.2015.11.077

[9] Sandeep Sharm, Jaiprakash Nagar (2020), “Intrusion Detection in Mobile Sensor Networks: A Case Study for Different Intrusion Paths ”, Wireless Personal Communications, DOI: 10.1007/s11277-020-07697-1

[10] Dilip Kumar AhirwarPrashantVermaJitendra Daksh (2012), “Enhanced AODV Routing Protocol for Wireless Sensor Network Based on ZigBee”, International Conference on Computer Science and Information Technology, http://dx.doi.org/10.1007/978-3-642-27299-8_11

[11] Kiran Kumar, T.V.U., Karthik, B., Improving network life time using static cluster routing for wireless sensor networks, Indian Journal of Science and Technology, 2013, 6(SUPPL5), pp. 4642–4647

[12] Thamarai, P., Karthik, B., Kumaran, E.B., Optimizing 2:1 MUX for low power design using adiabatic logic, Middle - East Journal of Scientific Research, 2014, 20(10), pp. 1322–1326

[13] T. Vijayan , M. Sangeetha , A. Kumaravel & B. Karthik (2020): FeatureSelection for Simple Color Histogram Filter based on Retinal Fundus Images for DiabeticRetinopathy Recognition, IETE Journal of Research, DOI: 10.1080/03772063.2020.1844082.

[14] D. S. Vijayan, A. Leema Rose, S. Arvindan, J. Revathy, C. Amuthadevi, “Automation systems in smart buildings: a review”, Journal of Ambient Intelligence and Humanized Computing https://doi.org/10.1007/s12652-020-02666-9

[15] Vijayan T, Sangeetha M, A. Kumaravel, Karthik B, “Gabor filter and machine learning based diabetic retinopathy analysis and detection”, Microprocessors and Microsystems,2020. https://doi.org/10.1016/j.micpro.2020.103353.

[16] Vijayan T, SangeethaM, Karthik B, “Trainable WEKA Segmentation of Retinal Fundus Images for Global Eye Disease Diagnosis Application,” International Journal of Emerging Trends in Engineering Research,Vol 8, No.9, pp. 5750-5754, Sep 2020. https://doi.org/10.30534/ijeter/2020/136892020

[17] C. Amuthadevi, D. S. Vijayan, Varatharajan Ramachandran, “Development of air quality monitoring (AQM) models using different machine learning approaches”, Journal of Ambient Intelligence and Humanized Computing, https://doi.org/10.1007/s12652-020-02724-2

[18] Vijayan T, Sangeetha M, A. Kumaravel, Karthik B, “Fine Tuned VGG19 Convolutional Neural Network Architecture for Diabetic Retinopathy Diagnosis,” Indian Journal of Computer Science and Engineering (IJCSE), Vol. 11, No. 5, pp. 615-622 Sep-Oct 2020. DOI: 10.21817/indjcse/2020/v11i5/201105266.

[19] Vijayan T, Sangeetha M, Karthik B, “Efficient Analysis of Diabetic Retinopathy on Retinal Fundus Images using Deep Learning Techniques with Inception V3 Architecture,” Journal of Green Engineering, Vol 10, Issue 10, pp. 9615-9625. Oct 2020

Bibliography

S.Rajesh, Research Scholar, Department of Electronics and Communication Engineering, Bharath Institute of Higher Education and Research Chennai, India. He has Completed M.E Applied Electronics in Sri Lakshmi Ammal Engineering College-Anna University. His research interests include Wireless Sensor Network, Networking, Cryptography. He is a member of IAENG.Email: *rajeshsports@gmail.com*

Dr.M.Sangeetha received the BE degree from the Bharathidasan university, in 1996, the ME degree from University of Madras, in 1999 and the PhD degree in Electronics and Communication engineering from Anna University in 2010. She is presently Professor of Electronics and Communication engineering, Bharath Institute of higher education and Research. She is also a member of IET and ISTE.Email: sang_gok@yahoo.com