11th International Conference on Recent Development in Engineering Science, Humanities and Management
Nutan Maharashtra Institute of Engineering & Technology, Talegaon Dabhade, Pune ESHM-18
24th-25th March 2018 www.conferenceworld.in ISBN : 978-93-87793-14-9

Detecting Intruder in Wireless Sensor Networks

Ashwini G. Sapkal[1], Prof. G.S.Ambadkar[2], Prof. S.V.Joshi[3]

[1,2,3]*NMIET,Talegaon-Dabhade, (India)*

ABSTRACT

The attacks occurring in Wireless Sensor Networks (WSNs) results in limiting or destroying the ability of the networks to perform its expected function. WSNs are networks which are having limited resources and can be deployed in unmanageable environments which can be easily accessed by an intruder or attacker. When an intruder attacks at network layer, it also affects the other layers. In the proposed work, Local sensor activity at multiple layers is monitored and evaluated to detect the possible intruder. A general methodology of an anomaly-based Intrusion Detection System (IDS), is modified (mIDS). mIDS uses the OTP (One Time Password) method, which are capable to discover the existence of intruder inside the network. Results shows that proposed algorithm has better End to End delay, Throughput and Packet Delivery Ratio.

Keywords—Packet Delivery Ratio, Security, Various Parameters, Wireless Sensor Networks.

I.INTRODUCTION

The unique characteristics of Wireless Sensor Networks (WSNs) made them attractive to be used in harsh environments. But the WSNs suffer from a various security attacks [1]. Security is very critical issue in case of WSNs. So, various security techniques are used in WSNs which can be classified as prevention and detection techniques [2] [3].The prevention techniques are used to ensure integrity and confidentiality and the detection techniques are used to detect the presence of intruder intervention in the network [4],[5].

A wireless sensor Network is a fundamental network which consists of sensing, computing and communicating with the components that gives an administrator the ability to instrument, observe and react to events and phenomenon in a specific environment [6].

1.1 Basic Sensor Network Elements

In this area, we briefly feature the fundamental elements ofsensor network as shown in fig. 1 below.

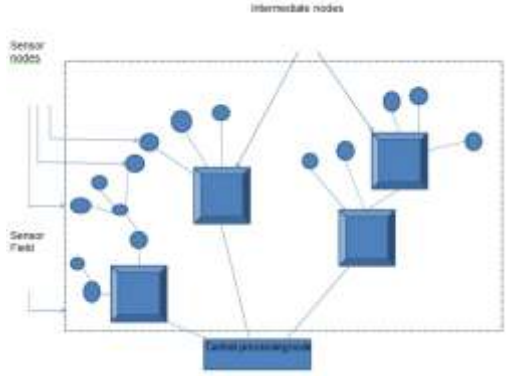

Fig 1: Architecture of WSN

A basic wireless sensor network is made up of number of sensor nodes which are densely deployed. They may be deployed in an open space such as on a battlefield, in the industrial machinery, at the bottom of a body of water, in commercial buildings, in a home or in or on a human body [7], [8]. The various sensor nodes are scattered in a special area called a sensor field. The data packets are transferred from source node to sink (destination) node. These packets are transferred through intermediate nodes and the central processing node as shown in fig. 1. Intermediate nodes allows the path to the sensor nodes to communicate with the central processing node .The figure shows the different shapes to categorise different types of nodes.

A sensor node has embedded processing and onboard storage capabilities .The node can have more than one sensor working in the acoustic, seismic, radio (radar), infrared, optical fields. Also it can works in chemical and biological domains. The node has communication interfaces which are wireless links to the neighbouring domains. The sensor node has not only location but also positioning knowledge which is achieved through a Global Positioning System (GPS) or local positioning algorithm. Each and every distributed sensor node has the capability to collect data, analyze and route them to the destination point.

II.RELATED WORK

The aim of Intrusion Detection Systems (IDS) is to monitor computer networks and systems. It detects all the possible intrusions in the network and alert users after intrusions are detected. IDS reconfigure the network if the system demands. The some recent developments in field of IDS systems for wireless sensor networks are discussed below-

1. Christiana Ioannou, Vasos Vassiliou and Charalampos Sergiou proposed [1] an Intrusion Detection System. According to authors, attacks in Wireless Sensor Networks (WSNs) results in limiting or destroying the ability of the networks to perform its expected function. In this paper they proposed a general methodology of an anomaly-based Intrusion Detection System (IDS) which uses the Binary Logistic Regression (BLR) statistical tool to classify local sensor activity to either normal or intruder. They evaluated the proposed system using routing layer attacks and they shown that mIDS is able to detect intruder activity within the range of 88%-100%.

2. Ilker Onat, Ali Miri proposed [2] an Intrusion Detection System for Wireless Sensor Networks with detection based security method. Though sensor nodes have low computation and communication capabilities, they have special properties like their stable neighbourhood information that allows for detection of anomalies in networking and transceiver behaviours of the neighbouring nodes. They had shown that such characteristics can be exploited as key enablers for providing security to large scale sensor networks.

3. Yousef El Mourabit , Anouar Bouirden, Ahmed Toumanari and Nadya El Moussaid proposed [3] Intrusion Detection Techniques in Wireless Sensor Network using Data Mining Algorithms. They presented comparative evaluation of the most preferment detection techniques in IDS for WSNs. Their results show that the random forest methods provide high detection rate and reduce false alarm rate. Finally, a set of principles is concluded, which have to be satisfied in future research for implementing IDS in WSNs.

4. Rodrigo Roman ,Jianying, Javier Lopez [4] said that the research of Intrusion Detection Systems (IDS) is a mature area in wired networks, and has also attracted many attentions in wireless ad hoc networks recently. In this paper, they discussed the general guidelines for applying IDS to the static sensor networks and introduce a new technique to optimally watch over the communications of the sensors' neighbourhood on certain scenarios.

5. Chung-Huei Ling, Cheng-Chi Lee, Chou-Chen Yang, and Min-Shiang Hwang proposed [5] a secure and efficient one-time password authentication scheme for WSN with algorithm that a user has authenticated over remote devices. It was designed to consider the limitations of computation and lower power in a wireless sensor networks.

III.METHODOLOGY

an anamoly based Intrusion Detection System|(IDS) , titled mIDS which uses the OTP (One Time Password) method is used. The proposed method is capable to discover the existence of intruder inside the organization. The anomaly Detection bases its conclusion on predictions, thus increasing the possibility of having sharp intruder rates. This problem can be overcome with proposed method.

3.1 MODIFIED IDS METHODOLOGY

An anomaly detection mechanism has the advantage of detecting unknown attacks, hence decreasing the false negative rate and has more false positive alarms. It requires offline training to determine the normal behaviour of the network and setting the certain limits or threshold which is used to characterise the normal behaviour. While on deployment the network activity is compared with the preset threshold and any deviation from what is set normally, is classified as abnormal or intruder.

Block Diagram

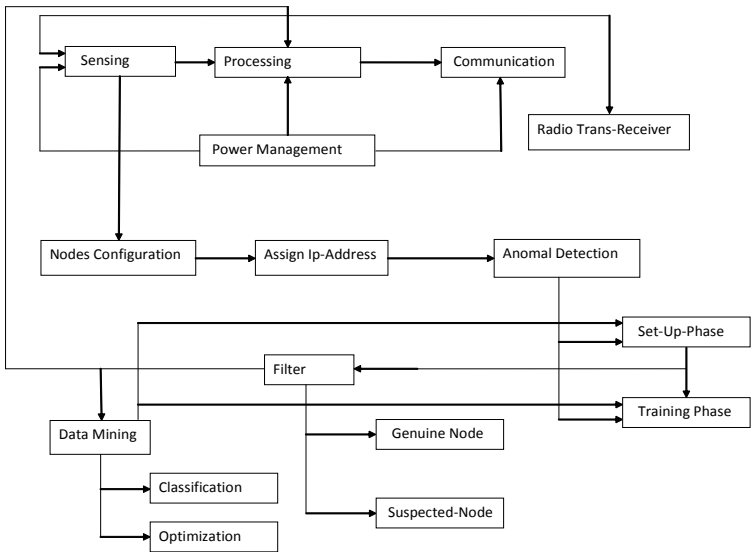

Fig 2: Block Diagram of mIDS system

Explanation:

Explanation of each and every blocks in fig. 2 can be explained as-

Sensing: sensor node sense the data and process the data and forward it to the intermediate nodes.

Power management: It includes transmission power and receiving power details.

Radio Trans-Receiver: Each sensor node can able to transmit and receive the messages.

Anomal detection: selfish nodes mitigate the performance of the network. So it affects the network performance such as packet ratio, throughput etc. we need to detect the selfish node by using Intrusion detection system.

Machine learning algorithm: which filter the data by using set up phase and training phase. Then it classify the node based upon the threshold value for genuine node and selfish node.

optimization: It selects the route which doesn't have any selfish nodes and process the data.

Flow Chart

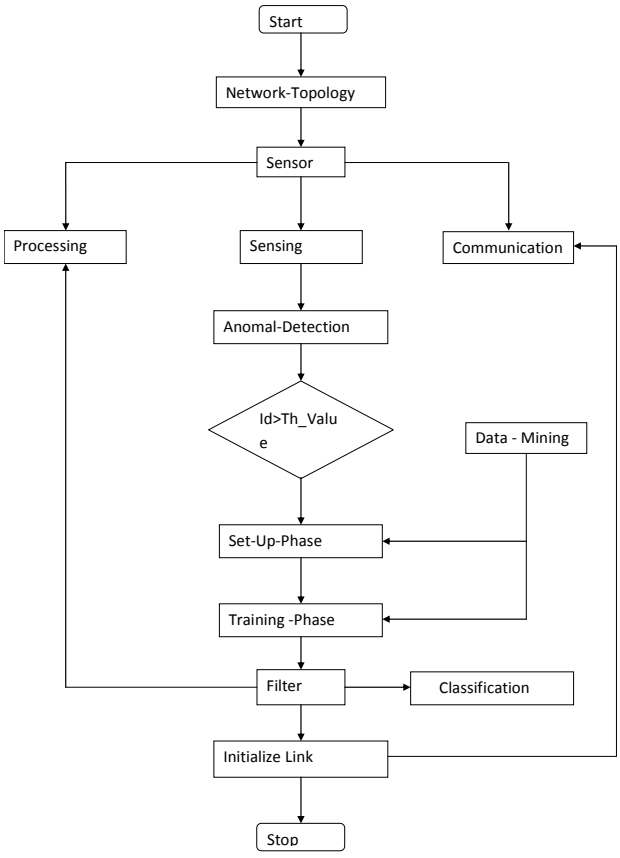

Fig 3 : Flowchart of mIDS system

Explanation of each and every blocks in fig. 3 can be explained as-

Selfish nodes catch the packet from source and doesn't forward the data packets to destination. So it degrades the performance of the network.Anomal detection is used to detect the attack by using filtering.Filtering is based upon set up phase,training phase.Classify the nodes based upon threshold value.Machine learning algorithm executes the above phases and process the filtering.The training set is randomly selected from the input data this step is called the learning step. This technique is very efficient and extensively uses classification of data by using MIDS.

IV.RESULTS

From the method we analyze the nature of network parameters of WSN. The following graph explains the performance of the network.

1.1 End to End Delay:

End to End Delay is the total time taken for a message to reach the subscribers from the publisher. In few cases, intermediate nodes in a network will lose packets. This may occurs due to errors while overloading of the intermediate network. The simulation results shows that our proposed algorithm have better End to end Delay than attacker performance as shown in below fig. 4.

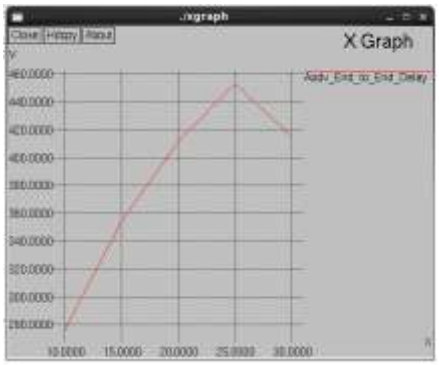

Fig 4: Analyzing number of nodes against end to end delay

1.2 Through-Put:

The total number of action executed or results to be produced per unit time. The amount of traffic which can be carried by a network is measured as throughput, usually in terms of kilobits per second. Throughput is analogous to the number of lanes on a highway and latency is analogous to its speed limit. PDR (Packet Delivery Ratio) is relative to throughput. The simulation results show that our proposed algorithm have better throughput as compared to throughput with attacker present in sensing network than attacker performance as shown in below fig. 5.

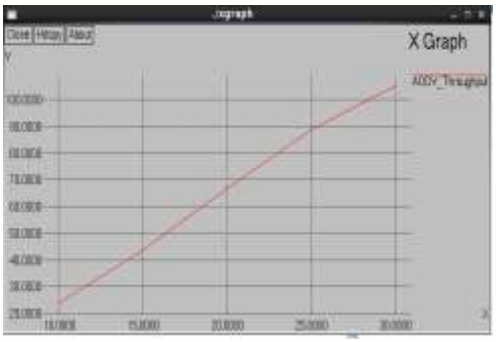

Fig 5: Analyzing number of nodes against through-put

1.3 Packet Delivery Ratio

The packet delivery ratio (PDR) is the total number of packets received by the destination nodes to the total number of packets transferred by the source nodes. The simulation results show that our proposed algorithm have better Packet Delivery Ratio than attacker performance as shown in below fig. 6.

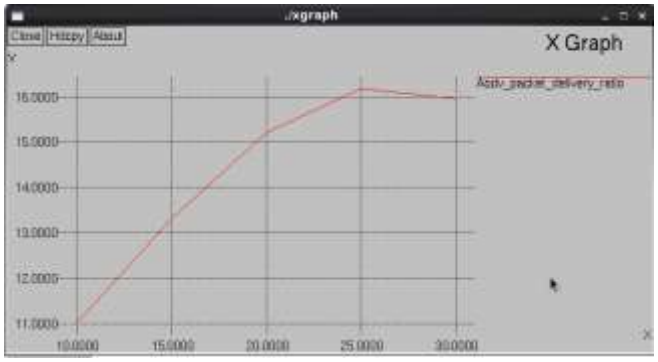

Fig 6: Analyzing number of nodes against packet delivery ratio

V.CONCLUSION

The major reason for the detection of attacker node is the loss of packet with time. As the time increases all the nodes lose their energy. The simulation results show that elimining attackers by proposed algorithm have better performance as compared to the network with attacker. It reduces delay and packet loss. The proposed method is used to decrease the effect of attacker. This detection approach is monitored by control node and process against the attacker nodes in the network. Simulation results show that the proposed algorithm has better packet delivery ratio, end to end delay and throughput.

REFERENCES

[1] ChristianaIoannou, VasosVassiliou and CharalamposSergiou, *"An Intrusion Detection System for Wireless Sensor Networks" 2017 24th international conference on Telecommunications(ICT).*

[2] IlkerOnat, Ali Miri ,"*An Intrusion Detection System for Wireless Sensor Networks"* , *IEEE international conference on wireless and mobile computing, networking and communications 2005.*

[3] Yousef El Mourabit , AnouarBouirden, Ahmed Toumanari and Nadya El Moussaid ,*"Intrusion Detection Techniques in Wireless Sensor Network using Data Mining Algorithms: Comparative Evaluation Based on Attacks Detection" International Journal of Advanced Computer Science and Applicatons, Vol. 6, No. 9,2015*

[4] Rodrigo Roman ,Jianying, Javier Lopez, *"Applying Intrusion Detection Systems to Wireless Sensor Networks"*

[5] Chung-Huei Ling, Cheng-Chi Lee, Chou-Chen Yang, and Min-Shiang Hwang ,*"A Secure and Efficient One-time Password Authentication Scheme for WSN" International Journal of Network Security, Vol.19, No. 2, PP.177-181, Mar .2017*

[6] G. Werner-Allen, K. Lorincz, M. Welsh, O. Marcillo, J. Johnson, M. Ruiz, and J. Lees, *"Deploying a Wireless Sensor Network on an Active Volcano," IEEE Internet Computing, vol. 10, Mar. 2006.*

[7] Basics of wireless sensor network by Rushin Shah, Feb 27, 2014.

[8] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, *"Wireless Sensor Networks for Habitat Monitoring," in Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications, WSNA '02, (New York, NY, USA), ACM, 2002.*