INTERNATIONAL JOURNAL OF ELECTRONICS AND COMMUNICATION ENGINEERING & TECHNOLOGY (IJECET)

ISSN 0976 – 6464(Print)
ISSN 0976 – 6472(Online)
Volume 3, Issue 3, October- December (2012), pp. 246-250
© IAEME: www.iaeme.com/ijecet.asp
Journal Impact Factor (2012): 3.5930 (Calculated by GISI)
www.jifactor.com

IJECET
© I A E M E

ENERGY EFFICIENT INTRUSION DETECTION SYSTEM FOR WSN

Syeda Gauhar Fatima, Dr. Syed Abdul Sattar, Dr.K.Anita Sheela

ECE dept., DCET, gauhar_sana@yahoo.com
#Prof.& Dean, RITS, Chevella, syed49in@yahoo.com
#Assoc. Prof ECE dept., JNTU, kanithasheela@gmail.com

ABSTRACT

Recently many new algorithms of wireless sensor networks have been developed which are mainly designed for wireless sensor networks where energy efficiency is an essential criteria. This paper describes a novel intrusion detection scheme which is a lightweight intrusion detection framework for clustered sensor networks. Since WSN nodes are typically battery equipped the primary design goal is to optimize the amount of energy used for transmission. The main idea behind using this approach is its communication and computation overheads are reasonably low and it performs better than other schemes in terms of energy efficiency and high detection rate.

1. INTRODUCTION

1.1 Wireless sensor networks (WSN)

Wireless sensor network (WSN) has become a very important topic with the rapid development that is vulnerable to a wide range of attacks due to deployment in the hostile environment. A WSN is a large network of resource-constrained sensor nodes with multiple preset functions, such as sensing and processing with number of low-cost, resource limited sensor nodes to sense important data related to environment and to transmit it to sink node that provides gateway functionality to another network, or an access point for human interface. These sensor networks are composed of energy constrained nodes embedding limited transmission, processing and sensing capabilities. Therefore network lifecycle becomes short and hence energy-efficient technique implementation becomes an important requirement for WSN. The WSN with coverage and connectivity have been implemented in many fields like Environment data collection where a canonical environmental data collection application is one where a research scientist wants to collect several sensor readings from a set of points in an environment

over a period of time in order to detect trends and interdependencies and then analyze the data. security monitoring are composed of sensor nodes that are placed at fixed locations throughout an environment that continually monitor one or more sensors at fixed locations through an environment that continually monitor one or more sensors to detect an anomaly node tracking scenarios used in tracking of a tagged object through a region of space monitored by a sensor network.[1][2][3][4]

1.2 Intrution Detection System (IDS)

Intrusion detection system (IDS) is a mechanism which detects malicious intruders based on those anomalies and attempts to monitor computer networks and systems, detecting possible intrusions in the network, and altering users after intrusions had been detected, reconfiguring the network if this is possible. These malicious intruders damage the important information while transmitting in wireless networks. Using detection system, the network will be able to respond and isolate the intruder in order to protect and guarantee its normal operation. Thus, Intrusion Detection Systems are crucial to safe operation in wireless sensor networks.
Two typical WSN IDS: collaboration –based Intrusion detection(CID) and Routing tables Intrusion Detection(RTID).Collaboration-based Intrusion Detection(CID) is a continuous intrusion detection system that detects intrusion during the cluster duty-cycle. Routing tables Intrusion Detection (RTID) is an event-driven Intrusion detection system. While the attacks are occurring, the IDS will compare the attack data and raise alarms.[4][5][6]

1.3 Issues of IDS in WSN

It is not possible for IDS to have an active full-powered agent inside every node in a sensor network. Each node is totally independent, sending data and receiving control packets from a central system called base station, usually managed by a human user.[7]

Without the IDS in WSN the threats can damage the network and consume large quantity of energy in monitoring suspicious nodes.

WSNs are composed of numerous low-cost and small devices, and are deployed into an open and unprotected area so they are vulnerable to various types of attacks.

The network lifetime decreases through utilizing the network's energy in a inefficient manner by malicious nodes.

1.4 Advantages Of IDS In WSN

Decreases Communication overhead since it is based on hierarchical structure of WSN.

The IDS techniques are lightweight science no training is involved and are depending on some strategies.

Controls the energy consumption from the malicious nodes in the WSN.

2. LITERATURE REVIEW

K.Q.Yan et al,.[8] have proposed an Intrusion Detection System(IDS) created in cluster head. The proposed IDS is an Hybrid Intrusion Detection System(HIDS).It consists of anomaly detection and misuse detection module. The goal is to raise the detection rate and lower the false positive rate by the advantage of misuse detection and anomaly detection module is evaluated. Wen Shen et al,.[9] have proposed a novel intrusion detection scheme based on the energy prediction in cluster-based WSNs (EPIDS).The main contribution of EPIDS is to detect attackers by comparing the energy consumptions of sensor nodes. The sensor nodes with abnormal energy consumptions are identified as malicious attackers. The advantage of this EPIDS is it is designed to distinguish the types of denial of service (DoS) attack according to energy consumption rate of malicious nodes. Tran Hoang Hai et al,.[10] have proposed a lightweight intrusion detection framework integrated for clustered sensor networks. And provide algorithms to minimize the triggered framework integrated for clustered sensor networks/And provide algorithms to minimize the triggered intrusion modules in clustered WSNs by using an over-hearing mechanism to reduce the sending alert packets. The advantage of this approach is it can prevent most routing attacks on sensor networks and less energy consumption in intrusion than other schemes. Edith C.H. Nagi et al,.[11] have proposed the architecture of hybrid scheme, authors have used combined version of anomaly and misuse detection techniques. In addition, they have also used cluster-based wireless sensor networks to reduce communication and computation costs. The advantage of this scheme is it performs better than other schemes in terms of energy efficiency and high detection rate.

3. PROBLEM IDENTIFICATION AND PROPOSED SOLUTION

In the paper [9] a novel intrusion detection scheme based on the energy prediction in cluster based WSNs (EPIDS) has been proposed. In this approach the malicious nodes are classified based on the energy consumption i.e, EPIDS first compares the energy prediction results with the actual energy consumption at the node and resulted malicious node will be put in the black list. In this approach sink node predicts the energy consumption of each sensor node and gathers energy residual of sensor nodes. The sensor nodes detect check their residual energy with the residual energy found by the sink node through a broadcast message. If the EPDIS detects abnormal energy consumed at a node then the node's ID will be put in a black list and will be removed from the routing table. The main drawback of this approach is that during the process of finding the malicious node ,the only thing considered is the energy consumed by that particular node which may not be sufficient enough to judge a node without considering the past of the node.

To overcome the above drawback we propose a hybrid Intrusion Detection System(HIDS) [8] which consist of anomaly and misuse detection module. This approach increases the detection rate and increases the false positive rate . This approach consists of three modules which considers the past of the node. This misuse detection module can be described in three phases. In the first phase ,the analysis of the network packets sent by the history and also the past packets that communicate on CH are collected to analyze, and finally the packets are divided into two types of normal and abnormal . In the second phase, the identification of Key are concentrated on features which are issued to distinguish between normal and abnormal packet.In the third phase the anomaly detection rules are established which are based on the

definition of a normal packet and the selected features, these rules are stored in the knowledge base.

In our proposal the nodes are classified through implementing EPIDS and calculate the residual energy and contain the node's ID, node's state. Based on these the nodes will be classified as a malicious or not. After classifying the nodes, the Hybrid Intrusion Detection System (HIDS) will be implemented where a past of node is considered which will be taken from the EPIDS. In the HIDS the packets sent by the malicious node are classified by the normal and abnormal. Initially the abnormal packets are converted into binary value and binary value is sent into the misuse detection module to calculate the output.

In this process the misuse detection module adopts a three- layer Back Propagation Network (BPN) which consists of an input layer, a hidden layer and an output layer. The number of processing units in the input layer is determined through the selected features for the packet. And the number of processing units in the hidden layer is designed through averaging the input layer units and the output layer units. The outcome of detection is sent to decision making module to integrate i.e., to the decision making module to detect the type of intrusion occurred.
The advantage of proposed approach is
Since the past of the node is been taken into consideration the intrusion detection will be done more effectively
And also the energy of the network will be increased and utilized in a efficient manner

REFERENCES

[1] . Tapolina Bhattasali,Rituparna chaki,"A Survey Of Recent Intrusion Detection Systems for Wireless Sensor Network", Advances in network security and applications, Springer,2011
[2]. T.Kavitha, D.Sridharan, "Security Vulnerabilities in Wireless Sensor Networks: A Survey", journal of Information Assurance and Security, vol. 5, p-031-044,2010
[3]. Olfa Gaddour, Anis Koubaa and Mohammed Abid, "SEGCOM: A Secure Group Communication Mechanism in Cluster-Tree Wireless sensor Networks",CommunicationsandNetworking,ComNET,3-6 Nov.2009
[4]. Shio Kumar Singh, M P Singh, and D K Singh, "Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks", International Journal of Advanced Science and Technology Vol.30,May,2011
[5].Ioannis Krontiris,Tassos Dimitrious,Thanassis Giannetsos, and Marios Mpasoukos, "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks", Algorithmic Aspects of Wireless Sensor Networks, Volume 4837,pp 150-161,2008
[6]. Rung-Ching Chen-Fen Hsieh and Yung-Fa Huang,' An Isolation Intrusion Detection System for Hierarchical Wireless Sensor Networks", JOURNAL OF NETWORKS",VOL.5,NO.3,MARCH 2010
[7]. Rucchi Bhatnagar, Dr.A.K.Srivastava and Anupriya Sharma," An Implementation Approach for Intrusion Detection System in Wireless Sensor Network", International Journal on Computer Science And Engineering Vol.02,No.07,2453-2456,2010
[8]. K.Q.Yan,S.C Wang,S.S Wang and C.W.Liu," Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-Based Wireless Sensor Networks", Computer Science and Information Technology(ICCSIT),3rd IEEE International conference,9-11 july 2010

[9]. Wen Shen, Guangjie Han,Lei Shu,joel Rodrigues and Naveen Chilamkurti," A New Energy Prediction Approach for Intrusion Detection in Cluster-Based Wireless Sensor Networks",Green Communications and Networking, Springer,Volume 51,pp 1-12,2012
[10]. Tran Hong Hai,Eui-Nam Huh and Minho Jo,"A Lightweight intrusion detection framework or wireless sensor networks",WIRELESS COMMUNICATIONS AND MOBILE COMPUTING,vol 10,pp-559-572,2010
[11]. Edith C.H.Ngai,Jiangehuan Liu and Michael R. Lyu,"An Efficiaent intruder detection algorithm against sinkhole attacks in wireless sensor networks",Computer communications,ELSEVIER,vol 30,pp-2353-2364,2007
[12]. Abror Abduvaliyer,Sungyoung Lee and Young-Koo Lee,"Energy Efficient Hybrid Intrusion Detection System for Wireless Sensor Networks",International Conference on Electronics and Information Engineering,2010
[13]. J Joy Winston and B. Paramasivan,'A Survey on Connectivity Maintenance and Preserving Coverage for Wreless Sensor Networks(IJRRWSN),Vol. 1,No. 2,June 2011