International Journal of Research in Advent Technology, Vol.7, No.5S, May 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Reactive Measures of Hierarchical Wireless Sensor Networks using Radial Basis Function

Dr.P C Kishoreraja
Department of Electronics and Communication Engineering SRM University, Delhi-NCR Sonepat,Haryana, India
pckishoreraja@srmuniversity.ac.in

Abstract—Wireless sensor networks are vulnerable to different types of attack as they are deployed in an unprotected and open region. In this research a Hybrid intrusion Detection system is proposed for a Hierarchical sensor networks. Proposed hybrid intrusion detection system, can detect intrusion in real time system by analyzing the attacks in different levels. Hybrid IDS includes a node based IDS (NBIDS) , cluster based IDS(CBIDS) and sink based IDS (SBIDS) which are designed for node level, cluster level and for base station. Different attacks are detected in various levels according to feasibility and probability of attacks

Keywords — Radial basis function; data Anomaly; selective forwarding; flooding; selfish misbehaviour; node replication; inkhole; performance analysis.

1. INTRODUCTION

Over the past few years, Wireless sensor network is one of the interesting research areas. The characteristics of sensor networks such as low cost, energy efficient, computational power, communication capabilities, multi-hop communication, distributed sensing and processing, dynamic network topology , self-organization expose the network to security attacks[1]. The main function of the sensor network is to gather the information from the surrounding environment and communicate to the sink. They are vulnerable to different attacks due to their deployment in open and unattended areas. The first line of defense, cryptography fails, when the attacker is inside the network. The second line of defense, intrusion detection system allows the detection of internal and external attacks. Considering the limitations, specific intrusion detection system is to be designed for wireless sensor networks [2]. Data transmission is the main concept in sensor networks, so most of the attacks are through route update misbehaviour. In hierarchical sensor networks, data sensed by sensors are aggregated in cluster head and communicated to sink by multihop communication. So in this paper different intrusion detection system is designed for sensor node, cluster head and base station. The paper is organized as follows; related work is presented in the next section. Section 3 proposed the hybrid IDS architecture for WSNs, algorithms and detection techniques against the routing attacks. Simulation and performance analysis is discussed in section 4.

2. RELATED WORK

Distributed detection process reduces the computational load of the system but increases communication overhead. The idea behind distribution in [3, 4] is that each sensor implements anomaly detection and transmits the summary to central location to construct a global model. Distributed model is designed based on kernel density estimator, a non-parametric statistical estimator [4]. Distance similarity measure calculated by each node detects the anomalies based on a common decision [5]. Statistical analysis [6] one-class principal component classifier (OCPCC) [7], candid-covariance free incremental principal component analysis (CCIPCA) [8] algorithm and dissimilarity of sensor observations in principal component space [9] are used to detect distributed anomaly. A hybrid algorithm used with Quantum PSO and RBFNN is implemented in [10], the convergence speed and precision of RBF based on immune recognition algorithm [11, 12]. Among various neural network based approaches RBF has good approximation ability, better classification and fast convergence [12]

A. Intrusion Detection System

The two categories of IDS are Host based IDS and Network based IDS [13]. Host based IDS evaluates the information available on a single or multiple host, where as in NBIDS, evaluation is carried out based on analysing the captured packets carrying information during network communication. The primary detection models to analyses the events are Misuse detection model and Anomaly detection model. Misuse model detects intrusion based on known signatures of specified attacks and Anomaly model detects intrusion based on abnormal network traffic.

Anomaly detection techniques are classified as Statistical techniques, Data mining and computational intelligence, Game theory concepts, Rule based techniques. Among the different intrusion detection techniques, data mining and artificial intelligence techniques has greater ability to gather similar traffic patterns in a cluster and isolate the uneven ones. One of the important parameter, feature selection, affects the performance of detection system. Decision making process and isolation depends on the clustering parameter selection. Security and performance metrics are always a trade-off while choosing an IDS technique.

With respect to the architectural design, Intrusion Detection System for Wireless Sensor Networks is classified as (1) distributed (2) Centralized (3) Distributed Centralized or Hybrid systems [14]. Most of the IDS are distributed where the attacks are detected locally by the sensor node. Major drawback is that the nodes should spend a significant energy to collaborate, communicate and overhear. Moreover a node has local knowledge about its neighbourhood and is unable to detect certain attacks. In centralized architecture design, the parameters and data for intrusion detection is to be transmitted to the sink or base station where there is a possibility of single point failure

and create large communication overhead. Hybrid IDS is the combination of distributed and centralized IDS.

B. Neural Network Approach

Through a set of processing units and interconnections between them, an Artificial Neural Network transforms a set of inputs to a set of searched outputs. Two types of neural network architectures are supervised training algorithms and unsupervised training algorithms. In the learning phase of supervised algorithms, the network learns the desired output for a given pattern or input, usually employed for pattern recognition problems. In unsupervised algorithms, the network learns without specifying the desired output, generally applied for classification problems [15]. The important characteristic of the neural network is that it automatically learns the coefficients, according to the inputs and outputs. During the training phase the network is exposed to normal data and attack patterns to adjust the coefficients automatically. Machine learning can detect both misuse and anomaly detection. The neural network approach reduced the false alarm and increased the detection rate.

3. HYBRID IDS ARCHITECTURE

The network model of the proposed hybrid IDS architecture is that the network is layered and clustered. Distributed IDS implemented in sensor node is the Node Based IDS, NBIDS, detects the data anomaly with respect the node. Based on mean variance the distribution of data is correlated and the anomaly is detected, Cluster Based IDS (CBIDS) in the monitor node (cluster head) detects the selective forwarding, flooding, selfish misbehaviour attack based on Radial Basis Function. Node replication attack and sinkhole attack is detected in base station using the same RBF architecture but based on different parameters as inputs.

```
Algorithm in NBIDS
If sensor sense data
    Store the data in table
    If table Qsize >Qthreshold
    Calculate μ, variance
        Calculate Data anomaly
            If Data anomaly<Dthreshold
                Drop
            Else
                Forward to CH
```

In CBIDS RBF is used for detecting the attacks, RBF structure has one input layer, 1 hidden layer and output layer. Input parameters are Packet dropping rate, number of data packets received, Packet forward rate, Forward delay time i.e. 4 input neurons. In the training phase, the range of all the parameters in the abnormal condition is fixed (by simulating the attack scenario) for each parameter, the centre of activation function and the spread factor is initialized for each range. Self-Organizing Map technique is used to initialize the centre and width factor. The choice of the parameters has an important influence on the classification performance 1. The number of neurons in the hidden layer. 2. The coordinates of the centre of hidden-layer 3. The radius (spread) of each RBF function in each dimension. 4. The weights between hidden & output layer. Proper selection of clustering parameters refine the isolation and enforce the decision making process.

Algorithm in CBIDS

```
Initialize number of center, initial co-ordinates
Initialize the spread parameter for each center
    Initialize the weights
        For each input vector
            For each epoch
                Calculate the output of each
node
                Cal error
            If error- minimum
                End for (epoch)
             Else
                Update the weight, Centre,
spread
            Do epoch
End for (input)
```

Sink Based IDS is implemented in base station to detect sinkhole attack and node replication attack. The input parameters to the RBF structure are packet Forward rate, Packet received rate, Node ID, Time location. With reference to the ranges Node Replication attack and Sinkhole attack is detected. Detection of attack and techniques is tabulated in table 1

Table 1.Detection and Techniques

IDS	**Techniques**	**Detection**
NBIDS	Rule based	Data Anomaly
CBIDS	Machine Learning - RBF	Selective Forwarding, Flooding Selfish Misbehavior
SBIDS	Machine Learning - RBF	Sink Hole, Node Replication Attack

4. SIMULATION AND PERFORMANCE ANALYSIS

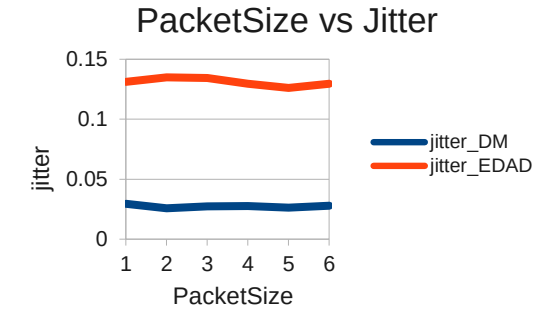
Simulation is carried out in NS2; Network Performance such as Throughput, Normalized OH, jitter, PDR is analyzed for variation in packet size and interval. IDS Performance such as detection ratio and false positive rate is analyzed for NBIDS for variation in number of attacker. The graphs are analyzed in fig.1. The data Anomaly is compared with the EDAD technique [10], from the graph it is analyzed that the data anomaly detection performance is improved and has reduced false positive rate and high detection ratio. Fig.2 shows the performance graph for Hybrid IDS architecture. It is observed from the graph that with HIDS the performance parameters are improved compared to without HIDS detection. Simulation parameters is tabulated in table 2.

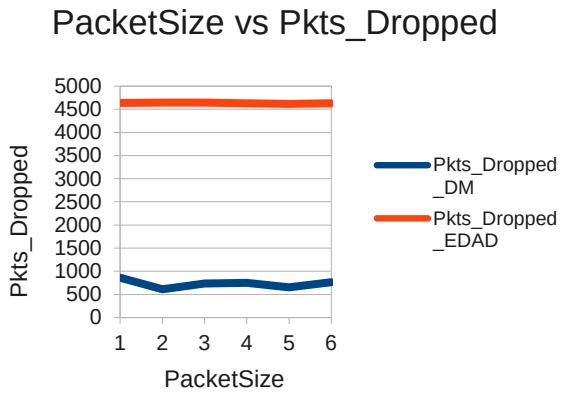
Table 2. Simulation Parameters

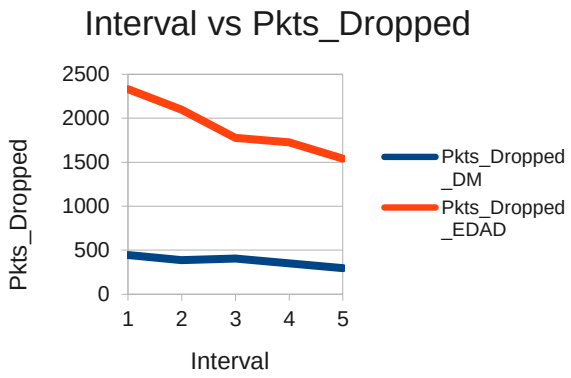
Parameters	**Values**
Total area	600 x 600
Number of Nodes	101
Total Simulation Time (seconds)	100
Routing Protocol	HIDS
Initial Energy(joules)	100
Interval	4 to 6
Attacker	1- 4

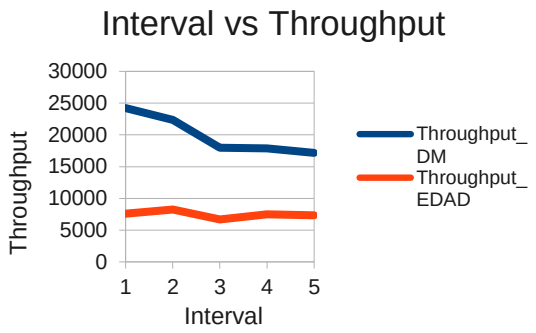
Packet Size(bytes)	50 to 100

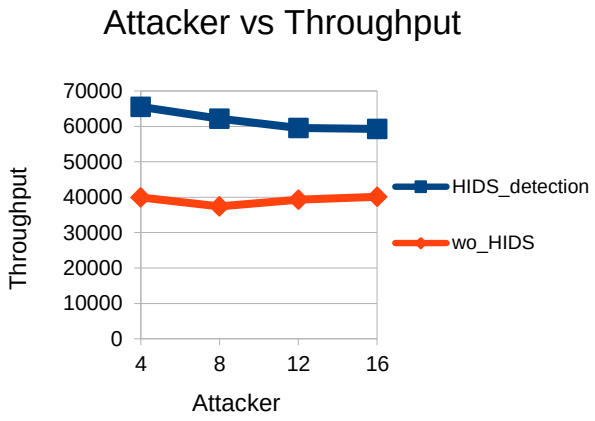
Fig 1. Performance graph for data Anomaly in NBIDS

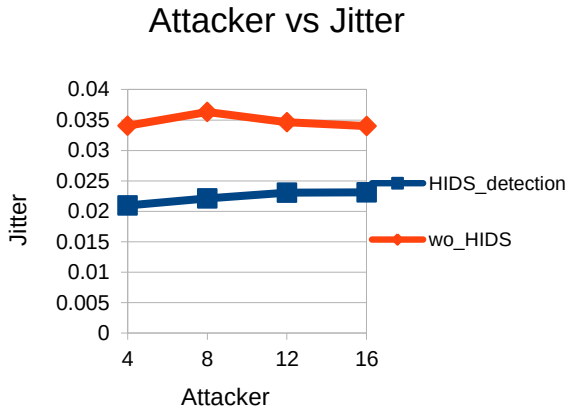


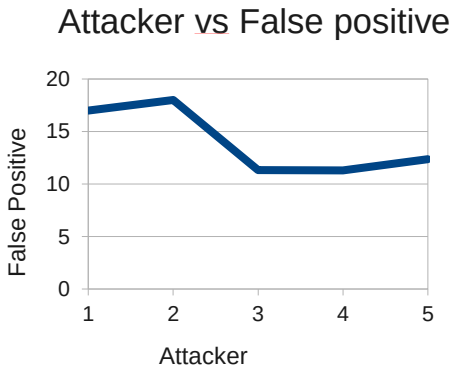












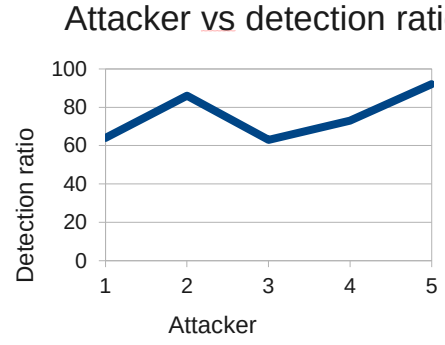


Fig. 2 Performance graph for Hybrid IDS Architecture

5. CONCLUSION

In this research Hybrid Intrusion Detection architecture is discussed for a hierarchical sensor networks. According to probabilities of attack, three IDS are designed for sensor node, cluster head, base station. Data Anomaly id detected n sensor node, selective forwarding, flooding and selfish misbehavior attack is detected in Cluster based IDS and node replication attack and sinkhole attack are detected in base station. Algorithm and parameters are discussed for Hybrid IDS. It is observed that the hybrid IDS has 92%detection ratio and 12% False Positive Rate. False positive rate can be further reduced by increasing the number of input parameters for Radial Basis Function architecture

REFERENCES

[1] Y. Maleh, A. Ezzati, "A review of security attacks and intrusion detection schemes in wireless sensor network", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 5, No. 6, December 2013.

[2] H. Sedjelmaci, S.M Senouci"A Lightweight Hybrid Security Framework for Wireless Sensor Networks", IEEE ICC, Sydney, 2014.

[3] Zhang Y, Meratnia N, Havinga P. An online outlier detection technique for wireless sensor networks using unsupervised quarter-sphere support vector machine. In International Conference on Intelligent Sensors, Sensor Networks and Information Processing, 2008.

[4] Palpanas T, Papadopoulos D, Kalogeraki V, Gunopulos D. Distributed deviation detection in sensor networks. SIGMOD Rec., 2003. 32(4);77-82

[5] Branch J, Szymanski B, Giannella C, Wolff R,Kargupta H. In-Network Outlier Detection in Wireless Sensor Networks. In 26th IEEE International Conference on Distributed Computing Systems, 2006.

[6] Zhang Y, Hamm N, Meratnia N, Havinga P. Statistics-based outlier detection for wireless sensor networks. International Journal of Geographical Information Science, 2012. 26(8);1373-1392.

[7] Rassam M.A, Zainal A, Maarof M.A. One-Class Principal Component Classifier for Anomaly Detection in Wireless Sensor Network. In 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN), 2012; 271-276.

[8] Juyang W, Yilu Z, Wey-Shiuan, H. Candid covariance-free incremental principal component analysis. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2003. 25(8); 1034-1040

[9] Murad A. Rassam, Anazida Zainala, Mohd Aizaini Maarof, An Efficient Distributed Anomaly Detection Model for Wireless Sensor Networks, AASRI Procedia 5 (2013) 9 – 14

[10] Liu, Yuan. "Qpso-optimized rbf neural network for network anomaly detection."Journal of Information & Computational Science 8.9 (2011): 14791485.

[11] Peng, Yichun, et al. "Application Study on Intrusion Detection System Using IRBF." Journal of Software 9.1 (2014): 177183.

[12] Yichun, Peng, Niu Yi, and Hu Qiwei. "Research on Intrusion Detection System Based on IRBF." Computational Intelligence and Security (CIS), 2012 Eighth International Conference on. IEEE, 2012.

[13] Devaraju, S., and S. Ramakrishnan. "Performance analysis of intrusion detection system using various neural network classifiers." Recent Trends in Information Technology (ICRTIT), 2011 International Conference on. IEEE, 2011

[14] Michael Riecker · Sebastian Biedermann · Rachid El Bansarkhani · Matthias Hollick, Lightweight energy consumption-based intrusion detection system for wireless sensor networks, Int. J. Inf. SecurDOI 10.1007/s10207-014-0241-1

[15] Ugur Halici. Artificial Neural Network. Chapter 9. Radial basis function Network .EE543 lecture notes. Metu EEE. Ankara 139.