Enhancing the Security of a Cluster-based Wireless Sensor Network Using Hybrid Intrusion Detection System

Mr. Tekchand H. Lonkar
ME 4th Sem (SSCET BHILAI)

Mr. Rajesh Tiwari
Asst.Prof. (SSCET BHILAI)
Dept. of CSE

Abstract— Advances in wireless communication and miniature electronics have enabled the development of small, low-cost, low-power sensor nodes (SNs) with sensing, computation and communication capabilities. Therefore, the issues of Wireless Sensor Networks (WSNs) have become popular research subjects. WSN is infrastructure based network, and through the mass deployment of SNs, a WSN is formed. The major function of WSN is to collect and monitor the related information which about the specific environment. The SNs detect the surrounding environment or the given target and deliver the data to the sink using wireless communication. The data is then analyzed to find out the state of the target.

1. INTRODUCTION

However, due to the design of their hardware, WSNs suffer from many resource constraints, such as low computation capability, small memory and limited energy. Two of the most common topology of WSN, Flat and Cluster-based Wireless Sensor Network (CWSN) [1, 19], are shown in Figure 1 and Figure 2 respectively.

Because WSNs are composed by numerous low-cost and small devices, and usually deploy to an open and unprotected area, they are vulnerable to various types of attacks. For example, when WSN is applied to the battlefield, SNs are invaded by the enemy and destroyed. Thus, the security of WSN needs to be considered. A prevention mechanism is used to counteract well-known attacks. It establishes a corresponding prevention method, according to the characteristics of an attack. However, prevention mechanisms cannot resist overall attacks. Therefore, the attacks are required to be detected. An Intrusion Detection System (IDS) is used frequently to detect the packets in a network, and determine whether they are attackers.

Additionally, IDS can help to develop the prevention system through acquired natures of attack.

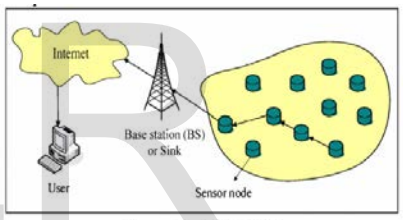

Figure 1. Flat WSN

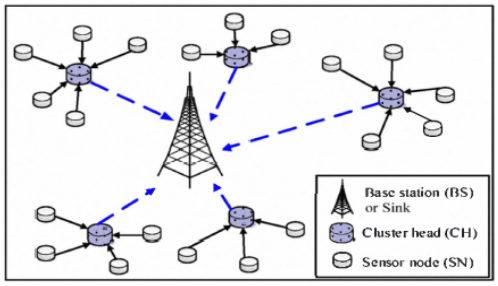

Figure 2. Cluster-based WSN

The IDS acts as a network monitor or an alarm. It prevents destruction of the system by raising an alarm before the intruder starts to attack. The two major modules of intrusion detection include anomaly detection and misuse detection [6]. Anomaly detection builds a model of normal behavior, and compares the model with detected behavior. Anomaly detection has a high detection rate, but the false positive rate is also high. The misuse detection detects the attack type by comparing the past attack

behavior and the current attack behavior. The misuse detection has high accuracy but low detection rate. Especially, the misuse detection cannot detect unknown attacks, which are not in the model base. Many researchers discuss the module of hybrid detection to gain both the advantages of anomaly detection and misuse detection [2, 7]. This combination can detect unknown attacks with the high detection rate of anomaly detection and the high accuracy of misuse detection.

The Hybrid Intrusion Detection System (HIDS) achieves the goals of high detection rate and low false positive rate. In this study, a HIDS is discussed in a heterogeneous CWSN. Cluster head (CH) is one of SNs in the CWSN but the capability of CH is better than other SNs [9]. Additionally, the CH aggregates the sensed data from other SNs in its own cluster. This makes a target for attackers. However, the CH is used to detect the intruders in our proposed HIDS. This not only decreases the consumption of energy, but also efficiently reduces the amount of information. Therefore, the lifetime of WSN can be prolonged.

2. PROBLEM DEFINITION

As Wireless Sensor Network consists of tiny sensing nodes which are deployed in a remote or hostile region, such as battlefield, it is prone to various types of attacks like jamming, hello flood, selective forwarding, sinkhole, Sybil, packet alteration etc.. In my observation it is found that existing Hybrid Intrusion Detection Systems cannot resist to the overall attacks and has some limitations like it has high false positive rate and low detection rate. Also, it cannot detect unknown attacks, which are not in the model base. Hence, it degrade the performance of the system.

3. OBJECTIVES

- To detect intrusion through packets in the Wireless Sensor Network and identify it as normal or abnormal packets.
- To identifying the type/nature of the intrusion/attacks by analyzing the abnormal packets.
- Finally to take the administrative action after reporting the types of the attacks to base station.
- To prevent destruction of the system by raising an alarm before the intruder starts to attack.
- To raise the intrusion detection rate and lower the false positive rate by the advantages of misuse detection and anomaly detection for enhancing the security of the system.

4. LITERATURE REVIEW

Hybrid Intrusion Detection System (HIDS) [1] filters a large number of packet records using the anomaly detection module, and performs a second detection with the misuse detection module when the packet is determined to intrusion. Therefore, it efficiently detects intrusion and avoids the resource waste. Finally, it integrates the outputs of the anomaly detection and misuse detection modules with a decision making module. This determines the presence of an intrusion, and classifies the type of attack. The output of the decision making module is then reported to an administrator for follow-up work. This method not only decreases the threat of attack in the system, but also helps the user handle and correct the system further with hybrid detection.

Wireless Sensor Network Security: A Survey [22], four main aspects of wireless sensor network security are observed: obstacles, requirements, attacks, and defenses. Within each of those categories there are sub-categorized the major topics including routing, trust, denial of service, and so on. The aim was to provide both a general overview of the rather broad area of wireless sensor network security, and give the main citations such that further review of the

relevant literature can be completed by the interested researcher.

In Efficient Approach to Detect Clone Attacks in Wireless Sensor Networks [5], Building a cloning attack detection protocol has some constraints. First, node locations must be learnt by other nodes (witnesses). Second, witnesses must be randomly associated to the scrutinized nodes to avoid security issues. They designed two new cloning attack detection protocols based on these constraints. They found that existing solutions have some drawbacks which greatly limit their usages, and then they explained the requirements to avoid the drawbacks. Based on these requirements, two protocols RWS and MRWS are proposed which are fully distributed and non-deterministic

An Intelligent Intrusion Detection System (IDS) for anomaly and misuse detection in computer networks is a novel Intrusion Detection System (IDS) architecture utilizing both anomaly and misuse detection approaches [2]. This hybrid Intrusion Detection System architecture consists of an anomaly detection module, a misuse detection module and a decision support system combining the results of these two detection modules. The proposed anomaly detection module uses a Self-Organizing Map (SOM) structure to model normal behavior. Deviation from the normal behavior is classified as an attack. The proposed misuse detection module uses J.48 decision tree algorithm to classify various types of attacks. The principle interest of this work is to benchmark the performance of the proposed hybrid IDS architecture by using KDD Cup 99 Data Set, the benchmark dataset used by IDS researchers. A rule-based Decision Support System (DSS) is also developed for interpreting the results of both anomaly and misuse detection modules. It is observed that the proposed hybrid approach gives better performance over individual approaches.

Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks [17], have illustrated MAC address based intruder tracking system for cluster based wireless sensor networks. This proposed system implements base station based detection and thus is very energy-efficient for early detection and prevention of security threats and attacks. Early detection and prevention of the intruder by efficient security system can prevent many problems like slowing down of the network, sending of fake data, etc. By designing a security system in which the Base Station (BS) keeps track of the security of the Wireless network, high security can be ensured without any significant energy overheads on individual nodes and cluster heads.

Neighbour-based intrusion detection technique in wireless sensor networks [14] is based on the principle that nodes situated spatially close to each other tend to have similar behavior. If a node does not tend to behave similarly to its neighboring nodes, it is considered an attacker. A neighbor based intrusion detection system is designed and implemented in this work. It is capable of revealing selective forwarding, jamming and hello flood attacks.

A secure group communication scheme [3] optimized the link layer communication of the wireless sensor networks. The scheme is independent of the underlying key management architecture. Scheme relies on clustering which divides the sensor field into control clusters with a cluster head in each cluster. Proposed local administrative functions LAFs imprinted with sensor node to achieve a high level security of node-to-node communication. LAF algorithm is efficient to establish a secure link layer communication. LAFs has the following properties: suitable anytime senders and receivers wish to guarantee integrity between sender and receiver, computationally very fast and very compact, accomplishes both of these properties with its reliance on a given hash function which are both fast and return compact outputs.

6. SYSTEM ARCHITECTURE

In CWSN, due to the heterogeneous nature of SNs, the capability of CH is greater than general SN. Additionally, because CH aggregates sensed data from

SNs, it therefore often suffers attack. The CH used to detect intruders is not only decreases the consumption of energy, but also efficiently reduces the amount of information in the entire network. The proposed HIDS in this research consists of three models is shown in Figure 3. The anomaly detection and misuse detection model is used to detect intrusion that to filter a large number of packet records using the anomaly detection model and to make a further detection with the misuse detection model. Finally, the decision making model integrates the outputs of anomaly detection and misuse detection models. It determines if an intrusion occurred, and classifies the type of attack. The output of the decision making model is then reported to the administrator for follow-up work.

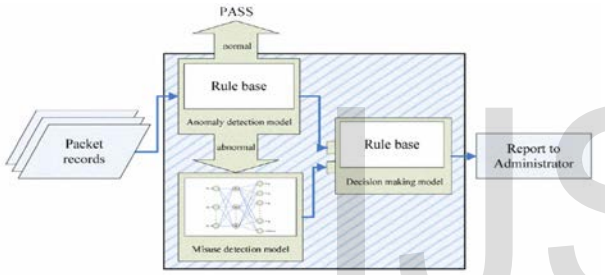

Figure 3. System architecture

An intrusion detection system (IDS) is necessary to detect the attacks. An IDS is able to detect packets in the network and determine whether it is intrusion or not. In order to get hybrid system, we use combined version of anomaly and misuse detection techniques. These techniques provide high detection rate and high accuracy of detection. In addition, use of cluster-based wireless sensor networks (CWSNs) to reduce communication costs and packet overheads.

7. RESEARCH DESIGN

A. Modules

1. *Anomaly Detection Modules*

The anomaly detection model plays a role like a filter in this research. Abnormal packets are delivered to the misuse detection model for further detection. Because the anomaly detection uses a defined model of normal behavior, a packet is determined to be abnormal by the system when the current behavior varies from the model of normal behavior. As a result, the anomaly detection usually determines the normal communication as abnormal communication, and creates the problem of erroneous classification. However, it seldom marks an abnormal communication as a normal communication. Therefore, the anomaly detection model is used to filter a large number of packet records first, and make further detection with the misuse detection model, when the amount of information decreases.

Our anomaly detection model adopts a rule-based method, using the rule base to analyze the packets, and distinguish which packets are abnormal. Therefore, a model of normal behavior is established. In our research, we use the rule-based method to construct the anomaly detection model. The flow of construction can be divided into three steps, as follows:

Step 1: **Analyzing the packet's historical records of CWSN.** In CWSN, the packets, which pass through CH, are sent from: (1) the member node of its own cluster; (2) the neighbor CH, which chooses this CH as the transmission path. Therefore, we collect the past packets which communicate on CH to analyze, dividing the packets into normal and abnormal.

Step 2: **Feature selection.** To find the features, which have identifiable properties, we compare the normal and abnormal packets to find the features, which determine normalcy, and develop the rules in our anomaly detection model.

Step 3: **Establishing the rules in anomaly detection model.** Because the anomaly detection determines attack occurrences, according to a defined model of normal behavior, we use the rule-based method to define the state of normal packets. The rules are defined, according to normal packets and the selected features. In addition, the defined rules are saved in a rule base. The established rule base is our anomaly detection model. In CWSN, all packets, which pass through the CH, have to be detected by

anomaly detection model. The misuse detection model makes further detection when it is abnormal. The detection flow chart of anomaly detection model is shown in Figure 3.

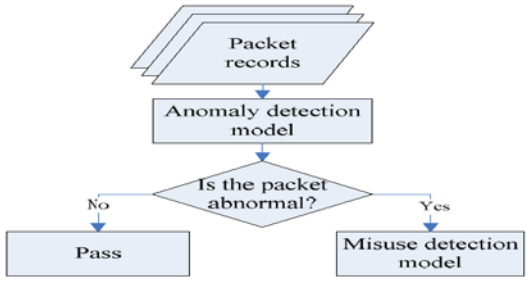

Figure 4. Flow Chart of Anomaly Detection Module

2. *Misuse Detection Module*

The misuse detection model utilizes various models of well-known attack behaviors, so we should build a model base according to these behaviors. In this system, we adopt BPN to construct our misuse detection model, because the performance in most techniques of intrusion detection is promised through training data. Through the supervised learning of BPN, learns the corresponding relations between input and output variables, and tunes the corresponding weight. It can result in the error for inference is minimal, so as to high accuracy. Therefore, BPN achieves high accuracy for our HIDS through mass trainings. We embed the model in the sensor when BPN has completed the training. In this research, a three-layer BPN is adopted for our misuse detection model that includes an input layer, a hidden layer and an output layer. We use the abnormal packets, which were determined by anomaly detection model, as the input vector. The number of processing units in input layer is determined through the selected features for packet. And the number of processing units in hidden layer is designed through the mean method, which is input layer units adds output layer units divided by 2. After analysis, we know that eight common attacks exist in WSN, including: Spoofed, Altered, or Replayed Routing Information, Select Forward, Sinkhole, Sybil, Wormholes, Denial of Service, Hello Floods and Acknowledgment Spoofing. Nine processing units in the output layer represent eight different attacks and one normal behavior, to determine whether the inputted packet is an intrusion, and make a classification.

We collect the packet's historical records, which pass through CH in CWSN, as the sample data for training. Most of packets are normal in WSN. This results in an unbalanced training data. In other words, when normal packets are too large, the BPN neglects the part which occupies a low rate data. In addition, to avoid this problem, we filter the training data through the anomaly detection model, and leave the abnormal packets for training. Before inputting the training data to BPN, we normalize the training data, and change it into a form, recognizable by BPN. In other words, we convert the packet records into binary values through preprocessing, and then input to BPN. The established flow chart of misuse detection model is shown in Figure 5. First, we set up the network parameters (we often get a better convergence when the learning rate is set to 0.5 or between 0.1 and 1.0. The actual learning rate is determined through simulation. Additionally, we assign values between 0 and 1 as the weights and biases

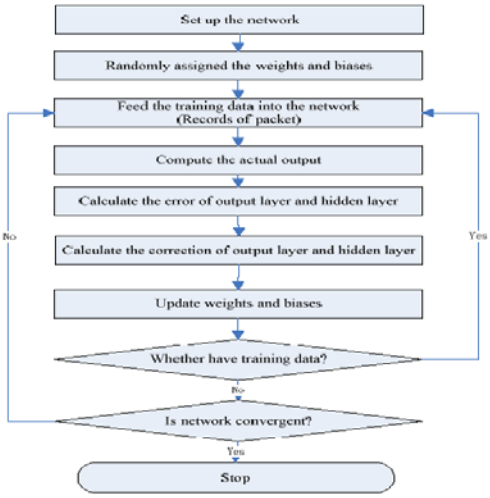

Figure 5. The Flow Chart of Misuse Detection Module

3. *Decision Making Module*

The decision making model is used to combine the outputs of the anomaly detection and misuse detection models. It determines whether or not an output is an

intrusion, and the category of attack. It then has to report the results to the administrator to help them handle the state of the system and make further corrections. We adopt a rule-based method to establish the decision making model, using the rules to combine the outputs of two detection models, and its main advantages are that it is very simple and fast. The rules of the decision making model are shown in Table I.

Rules
If anomaly detection model detects an attack **and** misuse detection model does not detect attack **then** it is not an attack and it is erroneous classification.
If anomaly detection model detects an attack **and** misuse detection model detects attack **then** it is an attack **and** determine the class of attack.

Table I. The Rules of Decision Making Module

B. Source of Data Collection

- Packet records are used as sample input to anomaly detection module.
- The simulated dataset is used as the sample to verify the performance of the misuse detection module.

C. Methods of Data Collection

- In this system, the data (packets) will sense with the help of sensors in the simulation. After that these packets will be stored or recorded in tables to the cluster heads and will get filtered by Anomaly Detection Module. Finally these packets will pass to the centralized security layer which will detect the attacks.

8. LIMITATIONS OF STUDY

There are following limitation of the research study

- The system is non deterministic
- The system has centralized approach
- The system will not be able to detect unknown attacks

10. POSSIBLE CONTRIBUTION

The possible contributions through the project in the Intrusion detection/Security in WSN as compared to previous approaches are as follow:

- The proposed system will decrease the consumption of energy.
- The proposed work will efficiently reduce the amount of information in the entire network.
- The lifetime of network can be prolonged by the proposed Hybrid Intrusion Detection System (HIDS).
- The system will enhance the security level and can detect more and more attacks.

REFERENCES

[1]. 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 Network", 2010 IEEE, pp. 114-118.

[2]. O. Depren, M. Topallar, E.narim and M.K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," Expert Systems with Applications, 29(4), 2005, pp. 713-722.

[3]. Maan Younis Abdullah, Gui Wei Hua, "Cluster-based Security for Wireless Sensor Networks", 2009 International Conference on Communications and Mobile Computing, pp.555-559.

[4]. Jiliang Zhou, "Efficient and Secure Routing Protocol Based on Encryption and Authentication for Wireless Sensor Networks", 2010 IEEE, pp. 406-409

[5]. D.Sheela, Priyadarshini, Dr. G.Mahadevan, "Efficient approach to detect clone attacks in wireless sensor", 2011 ieee, pp. 194-198.

[6]. F. Amin, and A. H. Jahangir, and H. Rasifard, "Analysis of Public-Key Cryptography for Wireless Sensor Networks Security," in Proc. World Academy of Science, Engineering and Technology (WASET), vol. 41, pp. 529-534, Montreal, Canada, May 2008.