Research on Intrusion Detection of Wireless Sensor Networks

Jianli Guo
Weifang University of Science and Technology,
Shouguang 262700, China

ABSTRACT

From the view of the wireless sensor networks data, this paper puts forward the sensing data mining based intrusion detection algorithm and intrusion detection of abnormal sensory data from the network protocol, node type, the system can not only apply to different wireless sensor network with good expansibility and general applicability, but also solve problems of a new hybrid heterogeneous network intrusion detection.

KEYWORDS: Wireless sensor network; Intrusion detection; Artificial immune system;

1 INTRODUCTION

Wireless sensor network is a distributed perception detection system by the deployment in wide areas of many sensor nodes, sensor nodes sense and monitor the area of information, the data transmitted to the sink node through multi hop routing, the sink node to reach the management node, realize the detection data acquisition and task. Because the node has the advantages of low cost, simple deployment, it cannot need to infrastructure and have strong survivability, high dynamic topology adaptation ability and other characteristics, wireless sensor networks has been widely used in multiple areas of vehicle monitoring, environmental monitoring, intelligent transportation, intelligent medical, military confrontation. However, due to the limited resource, wireless communication, interference, unattended and other reasons, wireless sensor network is facing severe security issues. The traditional encryption, authentication and other security protection technology for the security provides certain safeguards, but with the escalation of the means of attack, attackers have a breakthrough or bypasses encryption, authentication and other protective mechanism. So, it is urgent to study the security defence.

2 The methods of intrusion detection based on Internet of things

The Internet of things is the great development prospect in a new research direction. The network has many kinds of sensing devices, such as RFID (Identification Radio-Frequency) tags, sensors, actuators, mobile phones, etc.. The data types of its perception are very rich, and the amount of data is also very large, so it is necessary to analyze its data.. At present, the Internet of things is still in the exploratory stage of development, there is no mature network model can be used for reference, such as Figure 1 shows the three layer model is the generally accepted network model, including perception layer, network layer and application layer. The perception layer is the basis of the Internet of things, and different sensing devices constitute a heterogeneous network, and the wireless sensor network is also one of the many wireless networks in the perception layer.. Network layer mainly includes two aspects: transmission and processing, perception layer data via wired or wireless means (such as WLAN, WiFi, ZigBee, 3G, UMB) transmitted to upper server, the server of data aggregation of computing, storage and management, it describes the four main server. Application layer is mainly for the user, Supply server based on the network layer SCM (Chain Management), agricultural control, intelligent transportation, disease monitoring services.

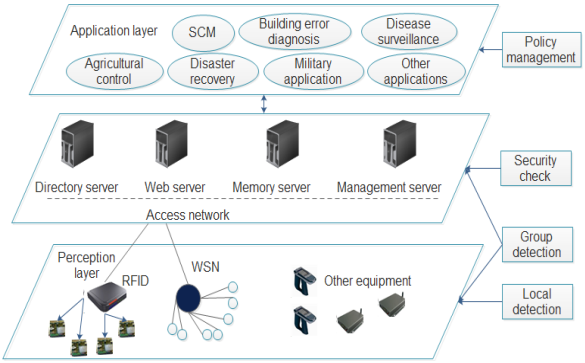

Fig.1 Data detection based on anomaly perception

Local detection module can be deployed in the perception layer of the sub network, the perceived equipment in sub network can gather local anomaly mining. The anomaly information can be transmit to the upper node through each communication channel; group detection module deploy in perception layer of the upper node (sink node) and the network layer device, global detection module deployed in the network layer device. According to different practical application, the configuration of different intrusion detection rules is issued and updated through policy management module.

3 Intrusion recognition based on anomaly mining

3.1 The analysis of intrusion behavior

The purpose of the intruder mainly includes: the network information, the destruction of the network normal communication, the tampering of the communication data and the network service cannot use. Analysis based on wireless sensor network layer attacks, attacks linked to wireless sensor network basic functions -- influence of environment monitoring data, we will invade behavior is divided into the following three categories.

(1) Data pollution: the attacker through the interception, forgery, tampering with the network packet, the false perception information sent to the sink node;

(2) Service Degradation: an attacker destroys the transmission of the packet or causes the transmission delay. For example, the packet delivery failed through the selection of forwarding or collision attacks, the transmission delay caused by retransmission attacks, resulting in service degradation.

(3) Denial of service: the attacker implemented the DoS class attacks, such as Ping/ICMP flooding, resource depletion, jamming, etc., resulting in network services cannot be used.

As can be seen, starting from the characteristics of the application layer, two kinds of information can be used to identify intrusion, a class is of abnormal sensory data, another is the data arrival rate, service degradation and denial of service are likely to lead to nodes that are not in accordance with the normal cycle to transmit data.

3.2 Intrusion detection rule

The anomaly mining algorithm can identify the hidden anomaly in the data, and how to detect the intrusion behavior from the anomaly is a problem need to be solved further.. In order to identify the occurrence and type of attack, combine the abnormal type and monitor the type of the physical attributes, formulate the IF-THEN rule to realize the detection.. Rule 1 is as follows:

Rule 1: IF (anomaly attri = sharp descent & property attri = voltage) THEN intrusion type = denial of service.

Among them, the "&" and "|" present logic "and" and “or", the semantic information of this rule is that occurs denial of service attack when the voltage value is suddenly dropped. From this rule, we can see that intrusion detection rule is simple and easy to expand, and the system can configure the appropriate detection rules according to its actual situation.

Through the analysis of the perception data, we propose a other general rule :

Rule 2: IF {{anomaly attri = sharp ascent &

property attri = humidity) & (anomaly attri = normal & property attri = temperature)) THEN intrusion type = data polluting.

This rule takes into account the relationship between different physical attributes, semantic information is that the data occurs pollution attack when the humidity dips and temperature data is normal.

In addition to these two rules, according to the actual application of the scene to configure more rules, and the module responsible for this feature is the policy management module. It can be seen that the proposed detection rule is not only flexible and scalable, but also good time and spatial association between different physical attributes.

3.3 Intrusion detection deployment

The anomaly mining of perceived data can be deployed to intrusion detection model, and it is dangerous to perceive nodes in the risk perception module. In addition, it can be deployed to the common hierarchical clustering network to improve the detection method in different types of network commonality. Literature [1] is hierarchical network structure, node will be the original data processing, the processed information (such as the radius) sent to the upper node for further detection, but these methods and the normal wireless sensor network function off, only to find out that noise, error and the surrounding environment in the event, not considered in the data fusion process data from tampering, replay and DOS attacks caused by abnormal, it is very difficult to find intrusion behaviors.

In order to realize the identification of intrusion, the test process in the paper distribute hierarchical cluster based network, as shown in Figure 2, the network are three kinds of nodes, common member nodes, cluster head nodes and the sink node. Cluster network is currently the most widely used and the most promising network structure, in the cluster network, the network self-organize into a plurality of cluster region. Each regional elections out of their cluster head, the common member nodes collection to the data after the data is sent directly to its own cluster head nodes, cluster head nodes to cluster data for fusion processing, forwarded to the sink node, usually cluster head has good resources. The intrusion detection method can be extended to the clustering network data fusion, to realize the intrusion detection.

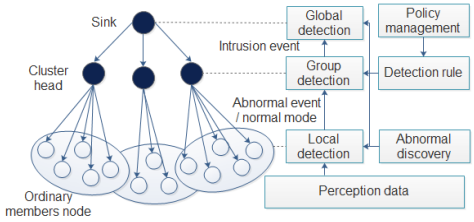

Fig.2 Intrusion Detection Based on anomaly mining of perceived data

The hierarchical detection process consists of the local detection module, the detection module and the global detection module. The local detection module is deployed on the common member node, the node collects the data regularly, runs the exception discovery algorithm, and sends the abnormal event four to the cluster head node when the discovery algorithm is found. This step can detect the exception of the local node, and when the node is awakened in the wake of the abnormal discovery function, do not need additional wake-up node running intrusion detection function. But in the local node suffer interference blocking, forwarding, node capture attack camouflage, physical destruction, will not be delivered on time abnormal event vectors, resulting in the upper nodes mistakenly believe that the network is in a safe state, so it is necessary to normal mode news reporting nodes periodically. On the one hand, the news to the cluster head nodes update their normal mode; on the other hand, if not duly received nodes of normal mode message, then the cluster head node can think network is subjected to the threat. Local detection can determine the occurrence of intrusion, but cannot identify the type of intrusion, group detection can solve the problem.

Cluster head nodethe can found same abnormality and run the test rules determine the occurrence and the type of the attack after sensing data received from member nodes, if the system judge that occurs attack, the cluster head node tissue invasion event vector is transmitted to the sink node, intrusion event vectors with the following five tuple:

The headid said detected intrusion of cluster head nodes, victimid said report the abnormal events in the cluster member nodes and the type of intrusion Intrusion_atrri table does not detect attacks, the same timestamp said does not detect the attack time, and {anomaly vectors set) that determine the attack by reference to the abnormal event vectors. Global detection module running in the sink node, main functions include further excavation of the intrusion event, determine the attack strength, coverage, to alert the management personnel, audit, management strategy.

4 Experiment simulation and analysis

As far as we know, there are no publicly known data sets of publicly attacked, so the perception of data come from the Lab Intel project. This project collected the environmental data in the Intel laboratory, including: temperature, humidity, light and voltage, once collect a data every 30 seconds, data record is about 23000000 perceived data.

Using OMNET++4.1 simulation software to form the cluster network, taking node 1, 16, 50 as three common member nodes, namely with the three node sensing data as the data analysis based, the node will be perceived periodic data transmitted to the upper layer node, the transmission cycle is 5 minutes. The network deployed an attacker, simulated data tampering attack, the attacker through the data intercepted member node, random data tampering.

4.1 Normal mode

Figure 3 is the temperature data of node 1, in which the solid line is time series by real-time acquisition and dashed line is the normal mode, you can see normal mode in constantly update, to adapt to changes in the bad environment, occurs in the absence of abnormal and almost real-time data on the perception of coincidence. After the exception, the normal mode stops the update and detects an exception.

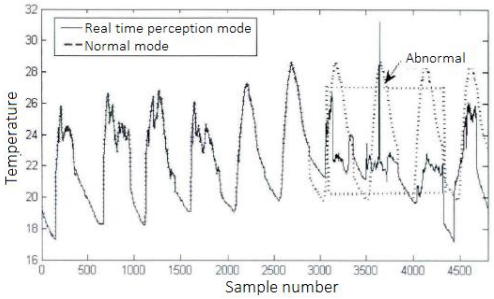

Fig.3 Normal extraction mode

4.2 Abnormal recognition performance test

We use the detection rate to measure the performance of algorithm, measure of persistence, changes in the mode of these with persistent abnormal types, including a large number of continuous abnormal data, so as the abnormal we will not abnormal in a number, but will abnormal events as an anomaly. The parameters of φ =0.5, =0.5, φ =10, using the numberα =4 of characters, the number m=8 of characters after symbol, first use δ =2.4. Table 1 shows that the outlier mining algorithm can detect data in the presence of abnormal, especially for identification of these abnormalities of the short pulse, surge, sag and persistent constant can achieve almost 100% detection rate.

Table1 Anomaly detect rate

Node		Short pulse	Surge	Sag	Continuous constant	Mode transformation
	Temperature	1	1	1	1	0.83
	Humidity	1	0.8	1	1	0.91
	Illumination	1	1	1	1	1
	Voltage	1	1	1	1	0.71
6	Temperature	1	1	1	1	0.8
	Humidity	1	1	1	1	0.86
	Illumination	1	1	1	0.98	0.75
	Voltage	1	1	1	1	0.65
0	Temperature	1	1	1	1	0.75
	Humidity	1	1	0.8	1	0.75
	Illumination	1	1	1	0.91	0.8
	Voltage	1	1	1	1	0.63

5 Conclusions

We make a quantify comparison between the algorithm and Rajasegarar[3] proposed clustering algorithm. Clustering outlier mining algorithm is the classic perception data anomaly detection algorithm, algorithms will be varied with the time series by fixed radius of clusters were grouped and then calculate the cluster average intra cluster distance, and to identify abnormal clusters by the k nearest neighbor method. The performance of the algorithm depends on the radius of the cluster W. In order to compare with the method proposed in this paper, we will have the w values from 0.02 to 4 for experiments and compare the best values for the detection performance. To be apply the algorithm on temperature data node 1, 16 and 50.

Because the clustering based algorithm can't recognize the abnormal types, as long as the algorithm can label the data as abnormal, it can determine the anomaly corresponding types. We is found the algorithm in this paper is better than in most types of abnormal recognition method based on clustering. The reason is clustering algorithm will be a time series as a whole to identify abnormal, does not consider the internal data of the time series of abnormal.

Reference

[1] Han Zhijie, Cao Xiaomei, Chen Guihai. The attack detection scheme of sensor network denial service based on traffic prediction [J]. *Journal of Computer Science,* 2007, 30(10):10-18.

[2] C. A. Carver. Intrusion Response Systems: A Survey [J]. *Department of Computer Science, Texas A&M University, College Station, TX,* 2000:77843-3112.

[3] S. Rajasegarar, C. Leckie, M. Palaniswami, and J.C. Bezdek. Distributed anomaly detection inwireless sensor networks[C].*Communication systems, 2006. ICCS 2006. 10th IEEE Singapore International Conference on. IEEE,* 2006: 1-5.

[4] Cui Zhiming, Gong Shengrong, Zhang Shukui, et al. Local control of virus infection in sensor network [J]. *Electronic Journal.*2009, 37 (4):877-883.