Research on intrusion detection algorithm for wireless sensor networks

Xianji Jin, Jingjing Wei, Weiming Tong *

School of Electrical Engineering and Automation, Harbin Institute of Technology, Harbin 150001, China

*Corresponding author e-mail: dianqi@hit.edu.cn

Abstract. With the gradual development of MEMS technology and the growth of network technology and communication bandwidth, the Internet of Things (IoT) has become the research favorite in the field of information technology nowadays. The sensor network, which integrates the three technologies of sensor, micro-electromechanical system and network, is a new information acquisition and processing technology. In the Internet of things technology to play the role of the information transmission expressway, although the Internet of things technology to achieve the interconnection of everything, but also triggered the advent of the era of big data, but in the massive data generation, data security has become an urgent problem to solve, and whether there is wireless sensor network information intrusion is also the focus of the research field. Based on the brief introduction of sensor network architecture, this paper analyzes and forecasts an intrusion detection algorithm in a valuable application field.

Keywords: Internet of Things technology wireless sensor network intrusion detection algorithm.

1. Introduction

With the development of Moore's Law, the computing power of Personal desktop computer (PC) is improved, the application of MEMS technology is complete and systematic, and the improvement of computing equipment with smaller size, lower price and more energy saving has laid the birth of an on-chip integrated System (SoC). At the same time, there is a lot of information transmission and processing structure, wireless sensor network is one of them. Wireless sensor network has been developed to realize the data collection, processing and transmission of three functions. So it and communication technology and computer technology together today constitute the three pillars of information technology. At the same time, massive data transmission will inevitably lead to information security problems, because wireless sensor network is often a dynamic data transmission mode, and traditional communication methods have a large difference in network security and detection has a large difference. Nowadays, in the field of information security and wireless communication, many scholars have done a lot of work on intrusion detection of wireless sensor network, this paper proposes a double-layer wireless sensor network intrusion detection algorithm, can reduce the intrusion detection system's attendance time and hardware cost.
2. Wireless sensor network

2.1. Definition

The Wireless sensor network (Wireless sensor Networks, WSN) is a distributed sensing network whose distal tip is a sensor that can perceive and inspect the outside world. Sensors in WSN communicate wirelessly, so network settings are flexible, device locations can be changed at any time, and wired or wireless connections can be made to the Internet. A multi-hop self-organizing network formed by means of wireless communication. The development of WSN benefits from the rapid development of MEMS (Micro-electro-mechanism system, MEMS), on-chip systems (System on chip, SoC), wireless communications and low-power embedded technologies.

![Figure 1. The Wireless sensor network system diagram](image)

3. Characteristics

(1) Large-scale network coverage In order to obtain accurate feature information, it is common to place large-scale sensor nodes in the monitored area, which can sometimes reach tens of thousands or even more than 100,000 orders of magnitude. The large-scale coverage of sensor network mainly includes two aspects: on the one hand, sensor nodes are distributed in a wide range of geographical areas, such as the use of sensor networks in the original forest protected areas for fire prevention, anti-poaching and environmental monitoring, because a wide range of sensor communication nodes need to be deployed; On the other hand,

Because of the high accuracy of location information, the sensor nodes are very dense, and a large number of sensor communication nodes are deployed in a small area of space. The large-scale coverage of sensor networks has the following advantages: the information obtained through different spatial perspectives has a greater price-to-value ratio; through distributed processing, a large number of acquisition information can improve the accuracy of monitoring and reduce the precision of single node sensor; the existence of a large number of redundant nodes makes the system have strong fault-tolerant performance, a large number of nodes can increase coverage of the monitoring area, reduce caves or blind areas.

(2) Self-organizing information collaboration In sensor network applications, where sensor nodes are normally placed without infrastructure, the position of the sensor nodes cannot be set in advance, and the neighbor relationships between the nodes are not known in advance, such as by seeding a large number of sensor nodes through the aircraft into the vast primeval forest, or arbitrarily placed in inaccessible or dangerous areas of the person.

This requires that the sensor node has the ability of self-organization, can be automatically configured and managed, and automatically forms a multi-hop wireless network system for transmitting monitoring data through topology control mechanism and network protocol. In the sensor network use process, some sensor nodes due to energy exhaustion or environmental factors caused the failure, there are some nodes in order to compensate for the failure node, increase monitoring accuracy and add to the network, so that the number of nodes in the sensor network dynamically increase or decrease, so that the network
topology changes dynamically. The self-organization of the sensor network can adapt to the dynamic change of the network topology.

(3) Dynamic nature

The topology of the sensor network may change due to the following factors: (1) or failure of sensor nodes due to environmental factors or exhaustion; changes in (2) environmental conditions may result in a change in the bandwidth of the wireless communication link, even when the time is off; the sensors, the perceptual objects, and the observers of the (3) sensor network may have mobility; (4) new node join. This requires the sensor network system to be able to adapt to this change, with dynamic system reconfigurable.

(4) Reliability

WSN is particularly suitable for deployments in harsh environments or areas where humans are not suitable, and nodes may work in open air environments, exposed to sun, wind, rain or even damage by humans or animals. Sensor nodes are often deployed randomly, such as by aircraft seeding or firing shells into designated areas.

These require a very robust sensor node that is not easily damaged and adapts to a variety of harsh environmental conditions. Because of the limitation of the Monitoring area environment and the large number of sensor nodes, it is impossible to manually "take care" of each sensor node, the maintenance of the network is very difficult or even non-maintainable. The communication confidentiality and security of the sensor network are also important to prevent the monitoring data from being stolen and obtaining false monitoring information. Therefore, the hardware and software of the sensor network must be robust and fault-tolerant.

(5) Data-centric the internet is the first computer terminal system, and then connected to become a network, the terminal system can be isolated from the network exists. In the Internet, the network equipment uses the unique IP address in the network, the resource location and the information transmission depend on the IP address of the network device such as terminal, router, and server and so on. If you want to access resources in the Internet, you first need to know the server IP address where the resource resides.

It can be said that the existing Internet is an address-centric network. Sensor networks are task-based networks, and it doesn't make sense to talk about sensor nodes out of the sensor network. The nodes in the sensor network are identified by the node number, and whether the node number needs the whole network depends on the design of the network communication protocol. Because the sensor node is randomly deployed, the relationship between the sensor network and the node number is completely dynamic, which shows that the node number is not necessarily related to the node location. When a user queries an event using a sensor network, it advertises the event of interest directly to the network, rather than to a node that determines the number. The network reports to the user after obtaining information about the specified event. This idea of the data itself as a query or transmission clue is closer to the habit of natural language communication.

So the sensor network is often said to be a data-centric network. For example, in a sensor network that is applied to target tracking, the tracking target may appear anywhere, and users who are interested in the target only care about where and when the target appears, and do not care which node is monitoring the target. In fact, in the process of target moving, it is necessary to provide the target location message by different nodes.

(6) Integration of The sensor node has low power consumption, small size and cheap price, which realizes the integration.

Among them, the rapid development of MEMS technology provides the corresponding technical conditions for the wireless sensor network contacts to achieve the above functions, in the future, similar "dust" sensor nodes will be developed.

(7) With dense node arrangement in the monitoring area where sensor nodes are placed, a large number of sensor nodes are arranged. By means of this arrangement, we can capture the spatial sampling information or multi-dimensional information, and achieve high precision target detection and recognition through the corresponding distributed processing. In addition, the accuracy requirements of
individual sensors can be reduced. After dense deployment of nodes, there will be a majority of redundant nodes, this feature can improve the fault-tolerant performance of the system, and the requirements of a single sensor has been greatly reduced.

Finally, some of the nodes in the appropriate sleep adjustment, but also to extend the service life of the network.

(8) Collaborative way to perform tasks this approach typically involves collaborative acquisition, processing, storage, and transmission of information. By collaborating, the nodes of the sensor can collectively realize the perception of the object and get complete information. This approach can effectively overcome the shortcomings of the lack of processing and storage capacity, and jointly complete the implementation of complex tasks. In the cooperative mode, the nodes between the sensors can realize the long distance communication, and they may be forwarded by multi-hop relay or through multi-node cooperative launch.

![Figure 2. The structure of the wireless sensor network](image)

(9) Self-organizing method the use of this mode of work is determined by the characteristics of the wireless sensor itself. Because the location of the wireless sensor node cannot be determined in advance, it is not clear its location relationship with the surrounding nodes, at the same time, some nodes in the work may be due to insufficient energy to lose utility, then additional nodes will be added to compensate for these failed nodes, and some nodes are adjusted to sleep state. These factors together determine the dynamic nature of the network topology. This kind of self-organization work mainly includes: self-organization communication, self-dispatching network function and self-management network, etc.

4. Intrusion detection method based on the characteristics of wireless sensor network

By analyzing the characteristics of wireless sensor networks, many intrusion detection algorithms are proposed and applied to wireless sensor network security detection. To date, many different types of attacks have been identified in wireless sensor networks, such as DoS attacks, spurious routing information attacks, selective forwarding attacks, black hole attacks, witch attacks, and halo flooding attacks. There are several intrusion detection algorithms based on feature and attack category:

4.1. Cooperative intrusion detection algorithm based on SVM mode and receiving power anomaly

Intrusion detection is the process of discovering, analyzing, and reporting unauthorized or damaging network activity. Demit and others [1] a self-organizing detection anomaly is proposed. Agar and others [2] a non-cooperative criticality and random learning intrusion detection scheme is proposed, which mainly utilizes the self-organization criticality of a certain regional environment variable and uses the hidden Markov model game method, the key is to find the most vulnerable node in the network and protect it. Silva and others [3] a distributed intrusion detection model is proposed, which is inferred from the event analysis of the Monitoring node. Liu et [4] An internal attacker detection scheme is proposed, which considers multiple attributes at the time of node behavior evaluation and does not require prior knowledge of normal or malicious sensor node activity; Li Guerue et al [5] a cluster-based intrusion
detection system is proposed, which divides the sensor network into several groups and then runs a group-based intrusion detection algorithm within each group.

The main scheme of the detection algorithm is as follows: This paper designs an intrusion detection module based on the Dos attack, halo flood attack, selective forwarding attack and black hole attack of wireless sensor network. Based on the SVM multi-class classification algorithm of binary tree, a five-class two-fork tree is constructed, as shown in Figure 3 and 4. The module can add sub-classifiers to detect new attacks, and extensibility is better.

Figure 3. Classification SVM two tree structure

Figure 4. Intrusion Detection Classification tree structure

This algorithm joins the activation algorithm of Intrusion detection module in sink node, looking for activating intrusion detects the node of the module. The algorithm is as follows:

At sink node assign \( U = \{ R \} \) //List of nodes in networks repeat
  For each node in \( U \) find MaxN (i) in \( U \) put in stack
  Assign \( U = U \backslash N (i) \) until \( U = \text{Null} \) send ID Sequels to nodes in stack
This algorithm assumes that the enemy is not able to successfully capture nodes in a very short network deployment phase.

At the same time, according to the abnormal reception power fluctuation to determine the timing of detection, to reduce maintenance costs, receiving power fluctuation anomaly mode is as follows;
Intrusion detection technology can be divided into two kinds of feature detection and anomaly detection. Feature detection assumes that an intruder's activity can be expressed in a pattern, and the goal of the system is to detect whether the subject activity conforms to these patterns.

The advantage is that the known intrusion can be detected accurately and effectively, the disadvantage is that it cannot detect the new attack, and the difficulty lies in how to design the pattern so that it can express the phenomenon of "intrusion" and not include the normal activities. Conceptually, an intrusion detection model mainly consists of two units [3, 4]: (1) features (attributes). Describes the characteristics of a typical activity, such as "Number of error entry attempts", "average frequency of command access". (2) Model algorithm.

Algorithms that use features for intrusion detection and intrusion suppression. The detection algorithm detects the intrusion pattern according to a certain rule, and the average received power (in DB) is chosen to characterize the behavior of the neighbor node. The algorithm takes the data packet count method based on the sliding window. In packets received by each node from the Neighbor node, only the last N packets are used to calculate the statistics of the Neighbor node packet, and each subsequent packet arrives and the statistic values are compared. N is called the packet main buffer length. If the packet conforms to the statistic value of the neighbor node, the packet is considered to be a normal packet and is used to calculate the new statistic value. The statistics value of the first packet is also cleared from the list. In the experiment, the arrival time and the receiving power of each arriving packet are recorded.

In order to monitor the received power of the exception packet, the minimum and maximum value of the packet receiving power needs to be constantly updated to match the received power value of each normal packet. The exception packet currently stored in the primary buffer of length N is either less than the minimum value of the normal received power or greater than the maximum value. Depending on the placement environment and application of the sensor network, the sensor network will issue an intrusion alert when a single exception packet is detected, or after a predefined number of consecutive packets are displayed as Exception mode. In the latter case, the exception packet must remain isolated from the normally arrived packet before the system takes some kind of decision. The buffer used to isolate the exception packet is called the intrusion buffer, and the length is defined as N 1.

Detection process for receiving power anomalies:

4.2. Receive the packet; According to the IDS rules to distinguish
If it is a normal packet, it is stored in the packet primary buffer if the packet primary buffer is not full, or in the exception buffer if it is an exception packet. 3) Alarm.

If the number of exception packets received continuously in the intrusion buffer is less than in 1, all exception packets are inserted into the packet master buffer, and if the number of exception packets received is equal to n 1, then in 1 consecutive packets are kept in the intrusion buffer and kept isolated from the normal packet, the system will issue an Intrusion Alarm.

If the system receives a normal packet after receiving an exception packet of less than N 1 consecutively, the intrusion buffer will be emptied. 4) Modify the IDS discriminant rule (that is, modify the statistical value of the model).

Modifies the IDs discriminant rule based on each insertion of an exception packet in the main buffer of the packet. The number of failed packets is called the fault threshold (Miss Threshold), whose length is defined as N 3. If there are n of abnormal packets that are not detected, the N packets will modify the characteristics of the packet's primary buffer and will not be detected again at a later time. Therefore, n 3 must be less than N.

Choosing the right n 1 and N 3 (the size of these values depends on the security vulnerability of the system) is critical because these values have a significant impact on the detection probability and the number of detections (which are mentioned in the next section). In the detection scheme for receiving power anomalies, in order to initiate a successful attack, the attacker must keep the relative distance between it and each neighbor node of the masked node basically intact. If the intruder is in a larger position, the probability of the packet being detected will increase due to the receiving power anomaly.
In order to invade the network, the attacker either uses the same hardware structure as the node transceiver or has power control to emulate the transceiver of the spoofed node.

![Figure 5. Power fluctuation anomaly algorithm detection effect](image.png)

5. Summary

According to the characteristic that the neighbor nodes in the network can provide stable information, this paper presents a method of anomaly detection based on the security mechanism of sensor network. If each node is able to establish a simple statistical model of the behavior of a neighbor node, these statistical models can be adopted to detect their changes. At the same time, according to the double-layer algorithm to dynamically monitor the security of wireless sensor network, the inner layer to do detailed screening, the outer layers do intrusion analysis. It is proved by practice that a node can effectively identify an intruder disguised as a legitimate neighbor node by analyzing the characteristics of a small number of packets received. In the implementation scenario, assuming that the anomaly detection algorithm runs independently on each node, a low-complexity collaboration algorithm may improve the process of detecting and deterring intrusions. Once an intrusion is found, the neighbor node will work together to divert the intrusion.

At present, the implementation of the scheme is not perfect, there are some detection errors and false alarm rate, improve the detection efficiency, reduce the false alarm rate will be the next step of the study of the specific objectives.

References

[1] Doumits, Agrawald P. Self-organized criticality& stochastic learning based intrusion detection system for wireless sensor network [C] //Proc of the IEEE Military Communications Conference. 2003: 609-614.
[2] Agah A, Dass, Basuk, etal. Intrusion detection in sensor networks: an operative game approach [C] //Proc of the 3rd IEEE International Symposium on Network Computing and Applications. 2004:343-346.
[3] Silvaa, Martinsm, Rochab, etal. Decentralized intrusion detection in wireless sensor networks [C] //Proc of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks.2005:16-23.
[4] Liu F, Cheng X, Chen D. Insider attacker detection in wireless sensor networks [C] // Proc of the 26th IEEE International Conference on Computer Communications.2007:1937-1945.
[5] Li Guo-Rui, He Jing-Sha, Fu Ying-fang. Group-base intrusion detection system in wireless sensor networks [J]. Computer Communications, 2008, 31(18):4324-4332.
[6] Wang Ying, Li Guoru. Packet-based intrusion detection scheme for wireless sensor networks [J]. Chinese Journal of Sensing Technology, 2009, 22 (6): 878-882.