Research on Fast Detection Method of Node Intrusion in Wireless Sensor Networks

Jieming Wu[1], Yi Zhang[2*]
[1]School of Mobile Communication, Guangdong Vocational College of Posts & Telecom, Guangzhou, 510630, China
[2]Guangzhou Branch, China Telecom Corporation Limited, Guangzhou, 510630, China

Abstract: With the continuous development of the Internet, Wireless Sensor Network (WSN) is also widely used in various fields, including forest protection, national defense, environmental monitoring, traffic management and other aspects. Meanwhile, there are also security problems. During WSN security research, the most critical is intrusion detection. Based on this, this paper first studies the characteristics of WSN and intrusion detection, then analyzes the main problems existing in the detection mode of WSN, and puts forward the corresponding optimization strategy.

Keywords: Wireless sensor; Network node; Fast detection of intrusion; Detection method

1. Introduction

With the development and progress of computer technology, information technology, network technology and electronic technology, sensor network has developed rapidly with its advantages of low power, low cost and portable. At present, sensor network can integrate information perception, information processing, data transmission and other functions in a small volume. With the acceleration of WSN research and the popularization of practical applications, many issues that had not been considered in the previous laboratory stage have been raised, such as node positioning of WSNs, network security and so on. For the security of WSNs, the requirements are different in different fields. In the traditional wired network, the research work of intrusion detection has been carried out for many years, and there are many mature achievements deserving to learn. But for WSN, the research of intrusion detection technology is in its infancy. Although some intrusion detection models and means based on WSN are put forward in the field of academic research, there is no universal detection model for wide application. Therefore, it is of great significance to carry out the research work on the detection method of network intrusion based on wireless sensor.

2. An Overview on the Related Sensor Intrusion Detection Technology

2.1. Intrusion of data link layer

Data Link Layer is between the physical layer and network layer. Data Link Layer provide services on the basis of the physical layer services. The basic service of the Data Link Layer is to input the data of original network layer into the adjacent node's target network layer secure and reliable. Because the Data Link Layer has a secure and reliable transmission of data characteristics, some bad people or organizations are to use their characteristics effectively. The characteristics have become a way to invade the sensor network. Unfair competition attacks, as well as collision and exhaustion attacks are typical of data link layer intrusions. A collision attack, when the wireless network is in an open physical environment, refers to that if two devices send and receive information at the same time, they can't effectively store and identify information by overlaying a signal. If any of data that existed in the data link layer appear unidentified situation, the entire packet will be discarded. Such shock behavior in the data link layer is understood as collision. In order to effectively avoid the emergence of collision attacks, in sending and receiving data, we can take error-correcting code or channel monitoring and transmission mechanism. The function of error-correcting code is to solve some low-quality communication channel data communication problems effectively. In correcting the error bit in the packet, some redundant information can be added to the communication packet. Collision attackers use instant attacks, but only affect individual data bits, so they can use error correction codes directly.

2.2. An analysis of misuse detection

Without detection and analysis is a more well-known knowledge of intrusion attacks. The establishment of the feature library and comparison on the characteristics of the library and data during work can detect the intrusion. First, through the knowledge of intrusion attacks that is

already in possession, a pattern for each intrusion or attack can be established, and then compare user behavior by establishing a pattern or multiple patterns. If the pattern that matches it can be found, then you can determine whether there are intrusion or attack behavior. Misuse detection belongs to a kind of feature library-based detection. If there is no characteristics of a behavior, the behavior can be called normal behavior. If this problem needs to be effectively solved, then we must continue to optimize the characteristic library update and perfect it. What way is used to optimize the characteristic library update is a difficulty factor. If the optimization feature library is updated through the WSN, then the larger energy will be consumed, and the WSN intrusion detection system low energy requirements are not consistent with the phenomenon. If the optimization feature library is updated by using recycled sensor nodes, it will be a large maintenance costs, and in certain specific situations it cannot be carried out. This series of problems will have a direct impact on the use of misuse detection methods in WSN intrusion detection.

3. The Key Problems Analysis of WSN Intrusion Detection Methods

3.1. Energy consumption

Because the sensor node is small in size, it is generally necessary to rely on a limited volume of button batteries as a storage device. Because the sensor has a large number of nodes, and it has a wide distribution area and geographical differences, some areas are not suitable for biological survival. When in the extension of node life human replacement battery is used, it feasible is not high. Carrying out automatic storage technology solar energy and other natural energy is not mature enough in China' development. Hence, through which way to effectively improve the use of limited energy efficiency is a key point in the WSN application development. Sensing modules and communication modules, as well as processor modules are modules in the energy consumption of sensor nodes. The power consumption of the sensing module is also gradually developing towards the direction of low consumption under the background of the continuous superbness of the integrated circuit technology city, and in the face of the continuous cumbersome upper-level application and the corresponding complex protocol, the computational energy level of the communication module and the processing module is growing geometrically, and the corresponding power consumption is also growing. As a high-level application system with WSN as the platform, the energy consumption problem is also an important bottleneck restricting its development. Among them, the selection of detection nodes and the intrusion detection algorithm of nodes need to be specially designed according to WSN to balance the energy consumption of nodes and the efficiency of system detection.

3.2. Performance issues

Sensor node belongs to a kind of micro-embedded device. Sensor node price and power consumption and other aspects are relatively lower than other nodes. These factors will also cause the sensor node to carry weak processor capacity, and its storage capacity is limited. However, in the context of the continuous wide range of WSN applications, sensor nodes must effectively complete a series of work, including data management and processing work and collection and summoning work in many aspects. Because the traditional intrusion detection system and operation has a large resource capacity, desktop or server based, in the traditional intrusion detection system, performance problems do not need to pay too much attention. The characteristics of the sensitivity of wireless sensor node energy consumption also represent the design of intrusion detection system with wireless sensor node as the main basis, which must be optimized on the basis of the limited processing power of the sensor node and storage capacity regulations. A single node in a WSN owing to its limited performance is not applicable in the centralized processing method. Coupled with the actual environment, the key nodes of the intrusion detection system are given to a node in an unknown geographical environment, such a low security, some not well-intentioned organizations, or individuals can analyze node traffic data size through the suspicious area, and determine its specific location, and then analyze the node internal data. And the entire intrusion detection system will be destroyed; even the entire sensor network will be damaged. In addition, a centralized processing method should be used. The system requires the collection of information throughout the network or the whole family. In the processing of data, it takes a long time, and a higher degree of malignancy nodes cannot be detected in a timely manner. Therefore, this way is not available.

4. The Solution on the Key Problems Facing by WSN Intrusion Detection Methods

4.1. Solutions to energy consumption problems

From beginning to end, the development of WSN is affected by the widespread development of energy consumption. It has also been clear in WSN operation process, upper-level applications and wireless communication and other aspects have higher energy consumption. The reduction in communication energy consumption is not within the scope of software optimization. Coupled with the communication energy consumption, the distance between communications is positively correlated. There is no area of WSN worth optimizing. Therefore, in the process of reducing energy consumption, the most

critical point is how to effectively improve the efficiency of node software processing. Intrusion detection system is to divide the cluster WSN into clusters and multiple detection groups. The nodes in the foot are not all used in intrusion detection. Every once in a while, only some nodes are selected as node detection and run detection algorithms. The main goal of this design is to effectively reduce the energy consumption of nodes. If each node in the cluster at the same time run detection algorithms, then the location of unlimited sensor network and monitoring of physical information forwarding and other aspects must adopt more processor resources. Coupled with detection algorithms it will also speed up the consumption of energy resources and shorten the time that nodes can use.

4.2. Performance problem solutions

In the traditional network environment, intrusion detection system from start to end has a relatively good detection performance. It has high accuracy rate and detection rate, false alarm rate and false alarm rate in the test environment. It can also be controlled within the scope. These are all due to the traditional network detection nodes which are not constrained by energy and processing power. In the face of wireless sensors such a limited energy, computing power is not too strong network node form. The design of intrusion detection system is particularly important. The design of the two-layer clustered wireless sensor intrusion detection system is proposed to solve the restriction of the limited node resources of the sensor network on the intrusion detection performance. In order to ensure a rapid response to intrusion behavior within the cluster, its main idea is to use lightweight intra-cluster detection algorithm based on Mars distance and to shield the obvious intrusion nodes directly within the cluster. And for those suspected intrusion nodes with high attack, covertness are reported to the nodes by the cluster head node. According to the suspicious address, the nodes in the network-wide listen for it, collect relevant information, and using a mature intrusion detection algorithm to detect the node again. If the detection results are normal, then notify all nodes of the network to stop the monitoring data of the suspect nodes sent, instead notify the isolation of the node.

5. Conclusion

In summary, one of the most promising and critical technologies in current is WSNs, which can be seen both in the military and civilian fields. WSN technology is still in the early stage of development. Under such circumstances, through what means to ensure that the network can always be in a safe state is the key point of WSN research. Whether in research or WSN security development, what can give full play to their role is the intrusion detection method. The existing wireless network sensor-based intrusion detection technology are optimized on the basis of traditional wired network and network security schemes. WSN itself has more characteristics of the difference, and does not apply to the field. Based on this, the characteristics of the existing intrusion detection technology and the characteristics of the WSN itself are analyzed, and further research is carried out on this basis.

References

[1] Zhang Wenyuan. Study on selective forwarding attack detection methods in WSNs. YanShan University. 2019.

[2] Zhang Zhihua. Research on key technologies for network intrusion detection of wireless sensors. Beijing University of Posts and Telecommunications. 2018.

[3] Su Qingsong. Study on the evaluation algorithm of cloning nodes in WSN based on ranging. Shenyang Aerospace University. 2018.

[4] Zhong Dunxuan, Zhang Dongmei, Zhang Yu. A WSN intrusion detection method based on similarity calculation. Information Network Security. 2016, (02), 22-27.

[5] Zhong Dunju. Research and realization of WSN intrusion detection technology based on similarity calculation. Beijing University of Posts and Telecommunications. 2016.

[6] Lu Fan, Wang Lijun. Research on WSN intrusion detection based on GA-LMBP algorithm. Laser Magazine. 2014, 35 (08), 36-40.