Research on Security Detection and Protection Mechanism of Internet of Things Based on Machine Learning

Xin Tang

School of Software, Zhengzhou University, 450002

Keywords: Security Detection. Protection Mechanism, Internet of Things, Machine Learning

Abstract: The Internet of Things is a new industry direction and a new stage in the development of information technology. At present, the Internet of Things is facing severe security threats, and the resource limitation of Internet of Things equipment further exacerbates its security problems. However, machine learning technology has inspired a new solution to the Internet of Things security problem. Based on machine learning, this paper analyzes the security problems faced by the Internet of Things at all levels, proposes the overall framework of the Internet of Things security system, and discusses the security management methods within the framework.

1. Introduction

The Internet of things has further expanded the scope of communication objects on the basis of traditional telecommunication networks and the Internet. It has expanded from people and people to things and things. It is committed to building a everywhere and everywhere network of "any time, any place, anything", and has developed a variety of business applications [1]. Machine learning, as a technology to realize artificial intelligence, can use different learning algorithms to realize the equipment training of non explicit programming. In the era of "big data", all kinds of information and data have become valuable resources that different interest groups are competing to mine, which leads to the problem of customer information disclosure and becomes a "disaster area" in the field of information security [2]. In today's triple play, the speed, security and accuracy of data exchange and processing directly affect people's quality of production and life. Intrusion detection system is widely used in traditional Internet. Industrial Internet of Things integrates Internet and industrial control network. Targeted application of intrusion detection technology can bring good security benefits [3]. After years of development, the Internet of Things has gradually been integrated into our life, making our production and life more intelligent and convenient. However, while the Internet of Things brings convenience to our life, it also faces more and more security threats. Therefore, it is of great practical significance to explore the application of artificial intelligence technology based on machine learning in the field of network security.

2. Overview of Machine Learning

Machine learning is a kind of learning that automates the calculation method of acquiring knowledge. Machine learning plays a very important role in the research of artificial intelligence [4]. In this process, according to a machine learning method, whether the sample in the input sequence has been marked as the title sample or not will be used as the training sample. Finally, a title extraction classification model is generated. Machine learning has developed into a multidisciplinary interdisciplinary subject in the past 30 years, involving probability theory, statistics, approximation theory, convex analysis, computational complexity theory and other disciplines [5]. Its application has spread to all branches of artificial intelligence, such as expert systems, automatic reasoning, natural language understanding, pattern recognition, computer vision, intelligent robots and other fields. Input sample instances are classified to determine whether they are a title. At the end of the extraction process, candidate titles selected by the classification model will also be screened [6].

Learn the rules from them, and then make decisions and predictions about events in the real world. Machine learning is different from software programs traditionally written to solve specific tasks. The main advantage of rule induction is that it has strong ability to process large data sets and is suitable for classification and predictive tasks. The results are easy to explain and technically easy to implement.

3. Classification and Analysis of Internet of Things Security Issues

3.1. Perceptual layer security.

The sensing layer terminal itself is vulnerable to external interference and damage. Most of the sensors are small in size and scattered. They are usually placed in exposed areas or places lacking safety protection and are vulnerable to human damage and theft. Telecom operators often find it difficult to carry out full identification, which leads to the inability to carry out full monitoring and risk detection in the first place when managing these customer information. As the perception layer will access the network layer, hackers will further attack the network layer through the perception layer as a springboard. Common attacks include intrusion infiltration, illegal access, denial of service attacks, etc. The sensing layer is based on a large number of physical electronic devices. The sensing layer of the Internet of Things monitoring system refers to the wireless sensor network of the monitoring system, which is composed of low-cost and low-loss sensor nodes located in the target detection area with data acquisition, storage, processing and transmission [7]. Network attacks have gradually evolved from individual hackers' tentative challenges to technology to behaviors with clear economic and political goals [8]. In addition, some early devices are still using very outdated software versions and cannot be upgraded remotely. The vulnerabilities and weaknesses of these software make Internet of Things devices very vulnerable to attacks. Communications between sensors and between sensors and networks are also vulnerable to eavesdropping. Even some nodes may be controlled and camouflaged, which may lead to information leakage or network collapse.

3.2. Network layer security.

Most of the information transmitted from the sensing layer is transmitted on the network layer in the form of IP packets. Although the existing communication network has relatively complete security protection capability, there are still some common security threats. According to the location of attackers in the network, such attacks can be divided into internal and external attacks [9]. In an internal attack, the attacker is one of the legitimate nodes. In the Internet of Things system, each Internet-connected object has a specific identification to realize interactive communication, and the number of these Internet-connected objects will far exceed the number of nodes in the Internet era. However, operators have more outlets in business halls, a large number of customer terminals, and a large mobility of service personnel. It is necessary to monitor the use and circulation of customer information from different levels.

RFID tags are an important part of the Internet of Things information system. They store a large amount of commercial value information, which is extremely attractive to illegal users and hackers. Once the information is leaked or tampered with, it will cause disastrous consequences. The schematic diagram of data theft and tracking is shown in Figure 1.

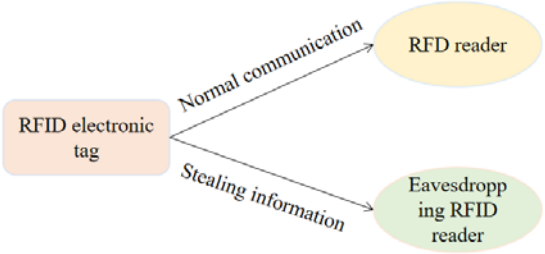

Figure 1 Data theft and tracking process

Data networks based on IP protocols have been found to have numerous security vulnerabilities and hidden dangers. Illegal intrusion, DDOS attack, network sniffing, Trojan horse virus and other traditional security issues on the Internet also pose threats to the information security of the Internet of Things [10]. These Internet of Things devices connected to the Internet have a large number of vulnerabilities. Attackers gain the default user name and password of the devices through the vulnerabilities, and then implant malicious software to infect and control these intelligent device systems. The security protection of network layer can draw lessons from the experience of traditional Internet and focus on the integrity and confidentiality of data. Industrial security gateway and intrusion detection technology can provide effective security.

3.3. Application layer security.

A large number of applications of the Internet of Things will bring massive data. The organization, analysis and processing of massive data require high data processing capability of the application layer. Once the capability is insufficient, it is easy to cause performance bottlenecks and data leakage. Under the given security level, the information system's comprehensive processing ability to resist malicious acts or unexpected events, which may endanger the storage, transmission and processing of data and information. This type of attack is classified according to the location of the attack protocol stack. For example, the data link layer can be attacked in the following ways: data flooding, legitimate nodes using carrier sense will face great collision probability when accessing the channel; Through industrial big data, data mining and other technologies to find the links that can be improved in the production and operation of enterprises, quickly and accurately capture valuable information and provide more and more intelligent decision support.

In addition to the method of data stealing from tracking, hackers can use man-in-the-middle attacks to intercept the interactive data information between the tag and the system. Illegal users access reader-writer equipment between the tag and the system. After stealing the identification information of the tag, they tamper with and destroy the data information and then transfer the reader-writer data. The whole process is reasonable. Schematic diagram of man-in-the-middle attack is shown in Figure 2.

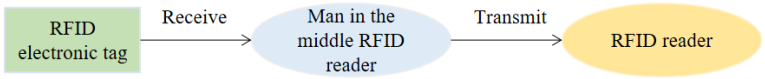

Figure 2 Man-in-the-middle attack process

Wireless sensor nodes will cause node failure due to weak communication signals, harsh basic environment and other problems, resulting in unreliable monitoring data. In order to ensure the reliability of monitoring data, it is necessary to adopt corresponding redundancy strategies in the monitoring area to make local nodes fail. At the same time, a large amount of data is stored in various business systems and platforms due to different application requirements. Data disaster tolerance, backup, error correction and synchronization between platforms need corresponding technical means to ensure. In the face of attacks, it is often difficult to be effective. When the hijacked Internet of Things device itself becomes an attacker, it is more difficult to detect and protect, which makes the availability, reliability and stability of the Internet of Things difficult to guarantee.

4. Security Detection and Protection Scheme for Internet of Things

4.1. Security detection scheme for internet of things.

Support Vector Machine (SVM) and Neural Network (NN) in machine learning can be used to detect DoS attacks in the medium access control layer. SVM and NN train the model according to two variables: collision rate and arrival rate. In NN, if the probability of DoS attack is greater than the preset threshold, DoS attack is considered to have occurred. When hackers try to attack a server, they often scan servers directly exposed on the Internet to collect necessary information. The information

real-time processing system of the application layer is mainly a terminal device that receives information at the server side, and realizes visual display, data query, mining, evaluation and future prediction of monitoring area data. A flexible and customized audit model is established by tagging log data to quickly support analysis of application scenarios such as personnel operation behavior portrait and behavior trajectory analysis. The hierarchical design of Internet of Things mainly starts from technology and functions, and defines the functions realized by each layer clearly. Personal privacy information is used by end users on a voluntary basis and by reaching agreements with Internet of Things operators, network operators and other suppliers as required. The embedded system based on Linux is simulated through a customized kernel, and IOCTL requests are forwarded to embedded devices running normally. For example, scan the server's ports to find out which services are open on the server and whether there are any defects or vulnerabilities that can be exploited. At the same time, it is also necessary to study the routing protocol of sensor networks and authentication between heterogeneous networks to prevent routing fraud and ensure the continuous, reliable and normal operation of networks.

Figure 3 shows the backbone transmission network with standby equipment, with RA as the main equipment reliability, Rb as the standby equipment reliability, and C as the network switching power. At this time, the reliability of the transmission trunk of the monitoring system consists of two parts, one part is the reliability Ra of the main equipment A in the transmission trunk of the monitoring system, and the other part is the reliability of switching to the standby equipment B and successful transmission when the main equipment A fails, which is C * (1-Ra) * Rb. The sum of the two is the reliability R1+1 of the transmission trunk of the entire monitoring system, and the calculation formula is:

$$R_{l+1} = R_a + c \times (1 - R_a) \times R_b \tag{1}$$

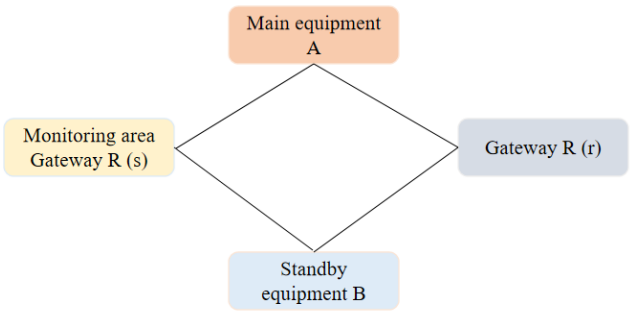

Figure 3 Backbone transmission network with standby equipment

Machine learning uses the statistical strength of data to discover potential patterns and knowledge, and provides interpretable results for further decision-making and automation. By sending various requests to a service port, analyzing its response data, and judging the version information of the software or operating system running the service according to its characteristics, machine learning attempts to attack through some special vulnerabilities in the system. Indirect anonymous information is used instead of real-name information to prevent the disclosure of personal privacy information and illegal activities or behaviors used by illegal users. In terms of network security, machine learning is one of the effective methods to detect network attacks and provide protection. Therefore, many researchers in the machine learning and security communities are committed to studying the algorithms and tools of automated security mechanisms. As the essence of scanning operations is that attackers send legitimate requests to servers, the server's response is used to judge or guess the server's information. Monitoring the stability of short-distance routing transmission data is poor, remote transmission data tampering problems and transmission lines are damaged, etc. Interruption of monitoring power supply equipment, interference of monitoring environment on data, and intentional or unintentional destruction by human will lead to unreliability of monitoring system. Some operational changes of users are found in advance and compared with the standard access path

in the existing knowledge base to predict the possibility of risks.

4.2. Security Protection Scheme for Internet of Things.

Aiming at the blocking attack problem faced by the Internet of Things, the current main scheme is to design according to the characteristics of different network protocol layers to avoid or prevent malicious interference attacks or reduce the degree of performance degradation when the network is blocked. However, it is difficult to clearly describe this difference by programming. At this time, it is the most suitable scene for the deep neural network to play its role. At this time, the data stream in the network can be used as the data input of the cyclic neural network. Grid deployment can achieve good coverage and connectivity. The sensor node completes data collection and transmits the collected information to the cluster head node through the node. The cluster head node fuses the data collected by the wireless sensor. In terms of physical layer countermeasures, radio frequency blocking attacks mainly use interference signals to prevent legitimate users from accessing channels or interrupt legitimate users' receiving signals. Therefore, a relatively simple anti-interference solution is to increase the power of the transmitter so as to improve the signal-to-noise ratio of the effective signals to achieve the purpose of anti-interference. Backpropagation learning model is used for training. Multilayer perceptron is composed of at least three layers of nodes. Except for input nodes, each node adopts neurons with nonlinear functions. There are few overlapping parts, high utilization rate of sensor nodes, and good energy-saving characteristics, especially for long-distance transmission, with obvious advantages.

Assuming that the relevant parameters Ci of both links are the same as 0.96 and the reliability Rc(i) of the communication function of the sensor node is 0.98, then the reliability R1 of information transmission to the cluster head node through link 1 is:

$$R_1 = \prod_{i=1}^{4} C_t R_c(i) = 0.752 \tag{2}$$

The reliability R2 for information to reach the cluster head node via link 2 is:

$$R_2 = \prod_{i=1}^{5} C_i R_c(i) = 0.700 \tag{3}$$

Assuming that the communication reliability Rc of each sensor node is 0.95, and the relevant parameters Ci are 0.96, 0.91 and 0.83 in turn, the data transmission reliability of sensor nodes in the transmission link is inversely proportional to the number of sensors passing by. when the information reaches the cluster head node, if wk >w, then the information is considered unreliable and discarded. At the same time, it reduces the task of cluster head node and congestion, as shown in Figure 4.

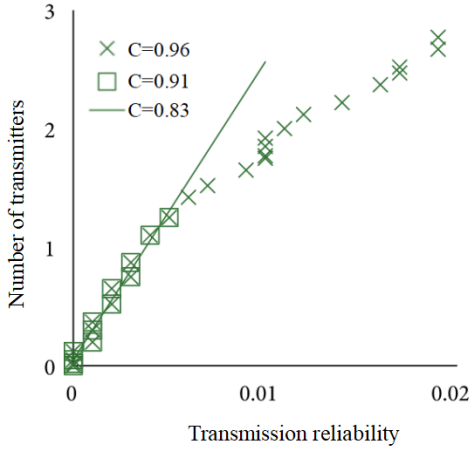

Figure 4 Relationship between number of sensing nodes and reliability

In the aspect of link layer anti-attack scheme, it usually depends on relevant protocols, and mainly provides active/passive protection through MAC protocol design to prevent interference attacks. Due

to the characteristics of cyclic neural network, it can well judge what operation the current data stream belongs to (normal access or malicious attack) according to the received data sequence, and then take necessary preventive measures according to the classification results. The sensor node will cover the monitoring area completely. At this time, there is no blind area in the monitoring area and the monitoring reliability is improved. The sensor node is deployed in the maximum range that the central cluster head node can perceive. The deployment method can also realize the full coverage of the monitoring area. However, TDMA protocol is very vulnerable to selective interference attacks because opponents can interrupt the victim's communication by simply interfering with their transmission slots. Machine learning methods can distinguish Internet of Things and non-Internet of Things devices based on data traffic. Sessions from each device can be used as a basis for classification, and category features can be extracted through different layers. If the cluster head node fails, the data of the whole monitoring surface cannot be delivered, so the cluster head node needs to take more effective measures to ensure its reliable operation. According to the probability given by the neural network, the administrator can intervene at his discretion, such as confirming authority, delaying response or even denying access.

5. Summary

The Internet of Things is a new industry direction and a new stage of information technology development. However, with the continuous development of the scale of the Internet of Things, the security problems it faces will become more complex. Artificial intelligence technologies such as machine learning and neural networks have played a role in many fields and penetrated into all aspects of our life and work. The Internet of Things provides users with convenient life experience through integration and processing of a large amount of information acquired through various sensors. Therefore, in the process of business development, it is necessary not only to pay attention to network architecture, technological evolution and business strategy, but also to take information security mechanism into consideration. Through quantitative analysis, this paper suggests that the sensing layer of the Internet of Things monitoring system should be deployed with regular hexagonal grids to achieve full coverage of the monitoring area, avoid the occurrence of monitoring blind areas and improve the reliability of the monitoring system. Based on machine learning technology, this paper puts forward the corresponding security protection countermeasures and practical experience for the Internet of Things, in order to make beneficial exploration for the Internet of Things operators in our country to realize all-weather all-round perception and effective protection of customer information.

References

[1] Antonini M, Vecchio M, Antonelli F, et al. Smart Audio Sensors in the Internet of Things Edge for Anomaly Detection[J]. IEEE Access, 2018, PP(99):1-1.

[2] Enshaeifar S, Barnaghi P, Skillman S, et al. Internet of Things for Dementia Care[J]. IEEE Internet Computing, 2018, PP(99):1-1.

[3] Caputo F, Scuotto V, Carayannis E, et al. Intertwining the internet of things and consumers' behaviour science: Future promises for businesses[J]. Technological Forecasting and Social Change, 2018, 136.

[4] Bradley R, Jawahir I S, Murrell N, et al. Parallel Design of a Product and Internet of Things (IoT) Architecture to Minimize the Cost of Utilizing Big Data (BD) for Sustainable Value Creation[J]. Procedia Cirp, 2017, 61:58-62.

[5] Chauhan J, Seneviratne S, Hu Y, et al. Breathing-Based Authentication on Resource-Constrained IoT Devices using Recurrent Neural Networks[J]. Computer, 2018, 51(5):60-67.

[6] Chincoli, Liotta M. Self-learning power control in wireless sensor networks[J]. Sensors, 2018, 18(2):375.

[7] Mershad K, Wakim P. A Learning Management System Enhanced with Internet of Things Applications[J]. Journal of Education & Learning, 2018, 7(3):23.

[8] Reid A R, César Raúl Cárdenas Pérez, David Muñoz Rodríguez. Inference of vehicular traffic in smart cities using machine learning with the internet of things[J]. International Journal for Interactive Design and Manufacturing (IJIDeM), 2017, 12(2):1-14.

[9] Kim J, Schiavon S, Brager G. Personal comfort models—A new paradigm in thermal comfort for occupant-centric environmental control[J]. Building & Environment, 2018, 132.

[10] Srinivasan S M, Truong-Huu T, Gurusamy M. Machine Learning-based Link Fault Identification and Localization in Complex Networks[J]. IEEE Internet of Things Journal, 2019, 6(4):6556-6566.