Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 9849025, 1 page
https://doi.org/10.1155/2023/9849025

Retraction

Retracted: Security Control Technology and Simulation of Network News Communication under the Environment of Internet of Things

Wireless Communications and Mobile Computing

Received 8 August 2023; Accepted 8 August 2023; Published 9 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] X. Zhou, J. Wang, and X. Zhou, "Security Control Technology and Simulation of Network News Communication under the Environment of Internet of Things," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 2730916, 10 pages, 2021.

Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 2730916, 10 pages
https://doi.org/10.1155/2021/2730916

Research Article

Security Control Technology and Simulation of Network News Communication under the Environment of Internet of Things

Xudong Zhou,[1] Jing Wang ,[1] and Xiao Zhou[2]

[1] *School of Journalism and Communication, Wuhan University, Wuhan, Hubei 430000, China*
[2] *China Unicom Henan Branch, Zhengzhou, Henan 450000, China*

Correspondence should be addressed to Jing Wang; wangjing93@whu.edu.cn

Received 26 April 2021; Revised 29 June 2021; Accepted 5 July 2021; Published 19 July 2021

Academic Editor: Keping Yu

Internet of Things is an application of network news communication technology. Based on the Internet, it uses physical access technologies such as radio frequency tag and wireless sensor network news communication and network news communication information transmission technology to build a network news communication information system that can cover people and things. In the physical layer, the relative position of the object is calculated by using multipoint cooperative localization, so as to determine the minimum anonymous region. Generate and maintain the anonymous tree topology on the network news dissemination layer, and provide storage management support for multiple anonymous groups. In the application layer, the object determines the corresponding anonymity degree according to the identity and uses the frame structure to construct and return the new anonymous group consistent with the existing anonymous group, which can prevent the persistent multiprecision query attack. A real-time control method for intrusion response of a security control system is designed, which includes two stages: response task generation and integrated scheduling. An intrusion response task set generation method based on an improved nondominated sorting genetic algorithm is presented, and a distributed integrated task scheduling and optimization algorithm based on a genetic algorithm and a directed acyclic graph is designed. The numerical simulation results show that this method can quickly and smoothly implement the response strategy of information security intrusion without affecting the normal execution of system tasks.

1. Introduction

With the development and progress of social economy, the Internet of Things has been applied in various important fields. Nowadays, driven by the development of various emerging technologies, such as the rapid development of Internet technology, network communication technology, and radio frequency technology, China's Internet of Things technology is gradually improving and progressing. IoT technology is no longer limited to the previous level and function but is now applied in a more extensive and detailed range [1]. The Internet of Things technology is involved in various aspects such as transportation, military, and financial fields. These fields are closely related to the development of a country. Therefore, only by doing a good job in network information security can the development of a country's economy be better guaranteed [2]. Analyzed at the technical level, the Internet of Things is similar to the Internet, so the information security problems existing in the Internet will also be reflected in the Internet of Things. The Internet of Things will be an important part of information transmission in the future, so it is very important to study the security control technology of network information transmission. The information security of the Internet of Things is a permanent topic in the research of the Internet of Things technology.

The IoT control system is widely used in rail transit, medical and health care, aerospace, industrial manufacturing, disaster, military, and other fields. However, the Internet of Things is a double sword; it brings convenience to people in the control system but also brings some security risks. For a long time, the control system in production and manufacturing industry is a closed and dedicated architecture. However, when the Internet of Things is combined with the control system, the control system will change from the original closed system to the open system, which is easy to be attacked by hackers, causing security problems such as secret leakage. Therefore, the control security in the Internet of Things environment could not be ignored.

At present, there are many methods to control network information security. However, through investigation, it is found that the existing control systems or methods all have certain limitations when facing the new characteristics of big data. For big data era of network information safety control work faces new situation, only the more practical and reasonable network information security control mechanism can ensure the safety of the huge amounts of data transmission and large database storage security, and only to establish perfect network information safety evaluation system can provide effective standard for network information security work.

2. Related Work

The perceptual layer is an important part of the Internet of Things, which is different from the Internet. The security research on the perceptual layer of the Internet of Things in academia is mainly to expand the existing work, such as data security in sensor network WSN [3], key management in the dynamic ad hoc network [4, 5], and authentication of RFID [6] and privacy [7]. But there is little work that involves various kinds of terminals and network after the integration of new scenarios (such as heterogeneous network integration of data transmission, without authorization, short interactive data interaction, and terminal capacity limited interaction), the security issues, or new problems arising from the Internet of Things (such as attacks of the attacker quantity dominant in the access network). Visual perception layer security issues involved in the information security are more complex than traditional, but due to the restriction of existing production cost and project income, sensing network has not been enough attention, such as Chen listed in the domestic Internet of Things mentioned in the standard [8] perception layer standard which is far less than the application layer and transport layer, also far less than the other two layers of related research work. It is necessary and urgent to study the security of a visible perceptual layer.

The current research on trust in the Internet of Things is not satisfactory. On the one hand, in the distributed environment, the existing trust model only focuses on a certain domain and lacks generality [9]. On the other hand, there is still a lack of research on the trust model specifically for the Internet of Things, so it is urgent to reunderstand and construct the trust model for the Internet of Things. For example, in the perception layer, Garau et al. believed that the trust mechanism had the following challenges [10]: (1) lack of facility support, (2) limited node resources, (3) fragile wireless channel, and (4) multisource.

There are the following challenges in establishing trust mechanisms for the Internet of Things: large-scale scenarios lead to unknown patterns of node interaction. Distributed environment makes the previous centralized security strategy for objects and terminals lose its effect. Heterogeneous environments make it impossible to use a uniform trust mechanism. Research on trust mechanism under the environment of Internet of Things is still quite deficient, and relevant research is not in-depth enough. There is a reputation evaluation system prototype [11] in the proposed security model of the Internet of Things, which includes the reputation management of perceived nodes, terminals, and users but does not include the reputation management of institutions. Obviously, the heterogeneous multisource nature of the Internet of Things will lead to malicious behaviors of institutions. In contrast, Rahim proposed the solution of the trusted Internet of Things [12] to study the trust relationship between institutions (EPCIs) with a sociological approach. However, they ignored the node trust in the perceptual network and did not consider the dynamic, heterogeneous, and large-scale characteristics of the underlying environment.

The Internet of Things is composed of various supporting technologies, such as object-oriented RFID communication, mobile computing for intelligent terminals, ad hoc network for sensing nodes, sensor network, and Internet-oriented service applications, social networking, and cloud computing technologies. The trust requirements of different subjects in these heterogeneous environments are also different. However, trust itself [13, 14] is a subjective and fuzzy concept, which depends on the interaction factors of subject, object, and environment [15]. There is no precise formal definition, and there is no single model that can accurately describe the trust value of subject, although there are some attempts to theoretically unify the trust between subjects in different networks [16]. But the concrete calculation model is not given. In addition, trust value is obtained through direct or indirect analysis of the attributes or behaviors of the subject, but if the interaction process of different subjects is different, it will bring great difficulties to the evaluation of trust value.

At present, the model-based fault recovery control method has been widely applied in distributed systems and autonomous computing fields [17, 18]. Vijayalakshmi et al. [19] studied the model-based adaptive self-healing system in autonomous computing, introduced the self-detection, self-reconstruction, and self-healing processes, and provided the types and recovery measures of software failures, the failure specification, and self-healing framework based on a model, and the aspect-based self-healing process and steps based on model. This paper studies the self-healing system based on the structural model, summarizes the basic elements that the dynamic fault repair system needs, describes the formal language of the structural model, gives the application tools and related technical specifications, and gives the self-recovery flow diagram of the system. In view of the software development of an embedded system and the application of the structural model, the structure description of platform-dependent and platform-independent parts is given, and the realization of instantaneous fault recovery of the structural model in an embedded system is introduced with application cases [20, 21]. Zavala et al. [22] introduce the requirement of structural model style for a self-healing system and the method of a self-healing system based on style. From these studies, it can be seen that the fault model construction in the general computing field is mainly based on the structural model, while the safety control field has more requirements on the management of the fault model and pays more attention to the safety and reliability at the system level.

In terms of the modeling and analysis of the safety system in the field of safety control, an in-depth study was conducted, and a Markov model was proposed to quantitatively calculate the reliability index of the safety system [23]. Aiming at the problem of fault detection in discrete time networked systems, a binary random sequence method is proposed to describe the random time delay of observation signals caused by networks [24]. A real-time reliability analysis and prediction technology was proposed to evaluate the reliability of equipment in use, which analyzed the reliability of equipment according to the input and output of equipment or state detection, and made real-time life prediction to provide technical support for the predictive maintenance of equipment [25]. At the same time, many researchers have studied the instantaneous fault recovery control problem based on a model. In the literature [26], an analytical model is proposed to deal with the sensor fault problem in the wire control system. Wen et al. [27] established a dynamic optimization method for cost assessment, combine multiple control objectives of the system, and comprehensively deal with actuator failures to ensure the stability of the wire control system. Other studies, from the perspective of controller design, enhance the robustness of the system and improve the ability to resist instantaneous failures, and put forward many control algorithms with fault-tolerant function [28–30]. The above studies have played a positive role in the development of fault-tolerant control, but most of them are based on the internal knowledge of some aspects of the system, so it is difficult to deal with instantaneous faults. Therefore, it is necessary to study the knowledge structure of the safety control system from the perspective of the system, build a model based on the characteristics of the system from the perspective of multiple fields, and then solve the instantaneous fault processing problem based on this "external" model. On the other hand, the fault-tolerant control of the security control system must also consider the problem of real time, and reasonable task scheduling is an important means to ensure the real time in the design of a networked control system.

3. Function Design of the Network News Communication Security Control System under the Environment of Internet of Things

3.1. Functional Safety Guarantee Structure Based on Instantaneous Fault-Tolerant Control. The security control system is a typical distributed structure, and its abstraction level can be divided into node level and system level [31–33]. The propagation directions of instantaneous faults in the safety control system are as follows: the propagation between components in the same abstraction level and the propagation from lower abstraction level to higher abstraction level. As mentioned earlier, transient failures occur at the node level and, if uncontrolled, will eventually propagate to the system level. Therefore, the best way to deal with it is to deal with all instantaneous failures in a timely manner at the node level. However, on the one hand, because the instantaneous fault type is changeable and the cause is complex. On the other hand, the node level needs a fast fault processing mechanism, which mostly adopts the fault knowledge-based processing mode. Therefore, it is almost impossible to handle all instantaneous failures at the node level. The hierarchical instantaneous fault-tolerant control structure of the safety control system proposed in this chapter is shown in Figure 1, including node-level components and system-level components. At the node level, the instantaneous fault is detected by the fault feature-based detection method, and the fault recovery is carried out by the preset recovery strategy. Faults that fail to be detected and handled at the node level (including unknown types of faults that fail to be handled and known types of faults that fail to be detected) will eventually affect the control quality or functional task structure of the system after the evolution of fault propagation. For this type of failure at the system level through the performance evaluation model based on the system and the function structure model of anomaly detection methods for testing, for detecting the abnormal, respectively, the fault-tolerant control based on sliding mode and system task allocation system with the method of reconstruction, realize the fault recovery, and ultimately guarantee the safe and stable operation of the system function.

At the node level, transient faults are divided into execution platform-dependent faults and application-dependent faults. The fault-tolerant control for the execution of platform-related faults is usually realized by the fault-tolerant control system embedded in the platform. Now, the microprocessor developers have relatively mature solutions for these kinds of faults. However, the application of related instantaneous fault needs to be considered in the design of a safety control system. In order to detect application-related instantaneous faults, Figure 2 presents the general representation methods of the state transfer model and data flow model of the safety control system. These states and data are selected according to the application design requirement specification of the intelligent node, which can directly reflect the characteristics of application-related instantaneous faults within the intelligent node.

3.2. Security Control Model of Internet of Things News Transmission against Bandwidth Consumption Attack. Figure 3 shows the WSN application scenario of security control. As can be seen from the figure, wireless sensor nodes collect equipment and surrounding environment information, connect with industrial core network through industrial access private network, and send the collected data back in real time and reliably. The application layer builds the application platform of various industrial businesses according to the specific application background of industrial control. Each application platform system provides fine-grained management and control on the basis of large amounts of data acquired by sensing means.

The main goal of the multilevel detection and early warning model of bandwidth consumption attack is to detect the

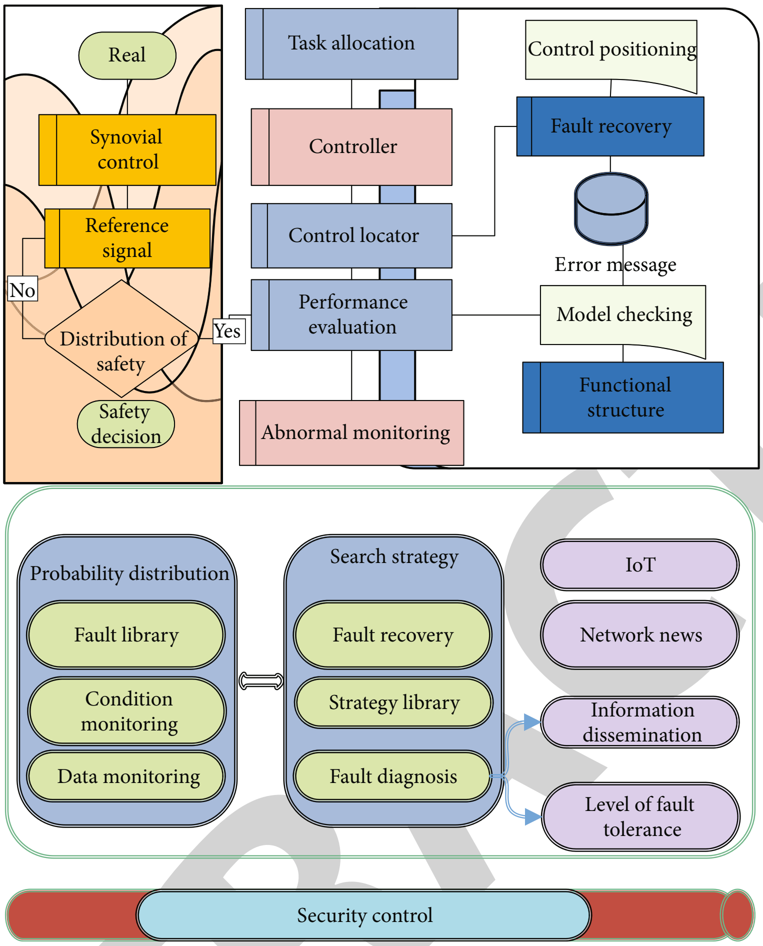

Figure 1: Hierarchy fault-tolerant control mechanism of network information communication security control system under the Internet of Things environment.

abnormal nodes attacked in WSN after the occurrence of bandwidth consumption attack, to give early warning according to the overall attack degree of WSN, and to take different levels of defense measures according to different levels of early warning information. Under this objective, the multilevel detection and warning model of bandwidth consumption attack must be able to complete the following functions:

The multilevel detection and early warning model system against bandwidth consumption attack must be able to detect the response time of nodes in WSN in real time and judge whether the nodes are subjected to bandwidth consumption attack according to the response time.

The multilevel detection and early warning model system for bandwidth consumption attacks should have multilevel early warning function. The system can count the number of nodes attacked in WSN and then infer the overall risk coefficient of WSN, judge the risk level, and finally give the corresponding warning tips.

The multilevel detection and early warning model system for bandwidth consumption attack should be able to take corresponding response measures according to the warning tips of different levels of WSN, so as to further expand the impact of antiattack, so as to ensure that the nodes can provide normal services to the outside to a certain extent.

In this section, a multilevel detection and early warning algorithm based on response time is proposed for bandwidth consumption attack in the WSN environment. In a multiple-level detection algorithm based on response time, monitoring device M plays an important role, the process of detecting early warning and the determination is done by the monitoring device M, and sensor nodes mainly auxiliary monitoring device M have done some related functions, such a design as far as possible to reduce the energy consumption of nodes and prolong the life span of the network.

The core idea of the algorithm is that the monitoring device M sends a request packet to the node in WSN at the time interval of T. The function of the packet is not only to return the total response time from the monitoring device M to the target node but also to calculate the node forwarding hierarchy and form the node forwarding hierarchy matrix. Obviously, the node forwarding hierarchy matrix changes with time. At the same time, the monitoring device detects the response time in the node forwarding hierarchy matrix, determines whether the sensor node is attacked by bandwidth consumption, and gives different levels of warning

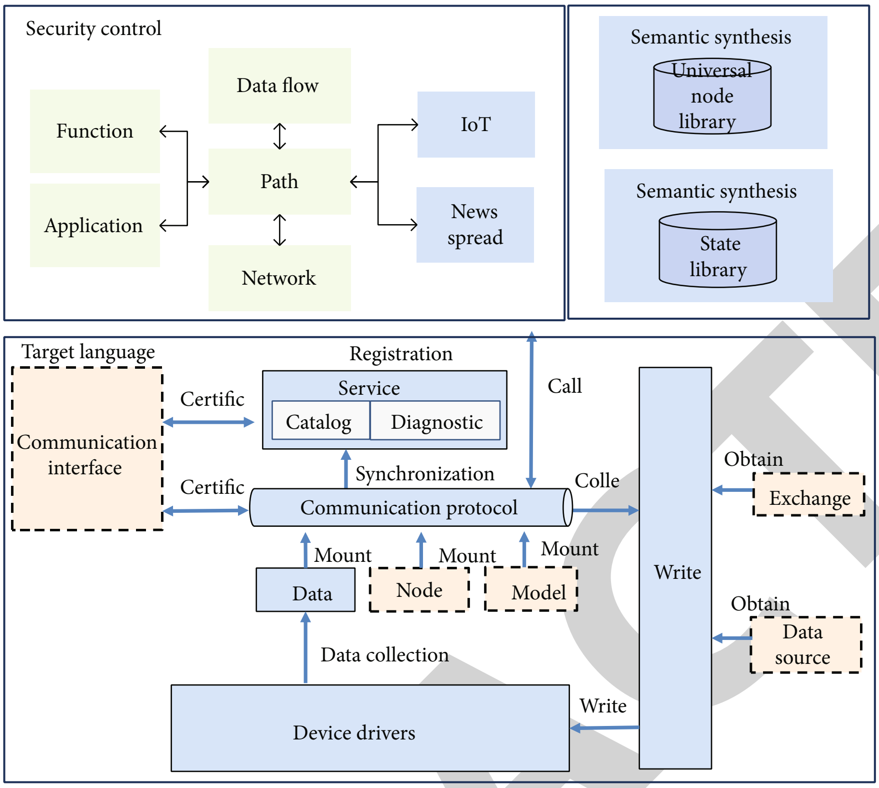

Figure 2: General node model of the security control system.

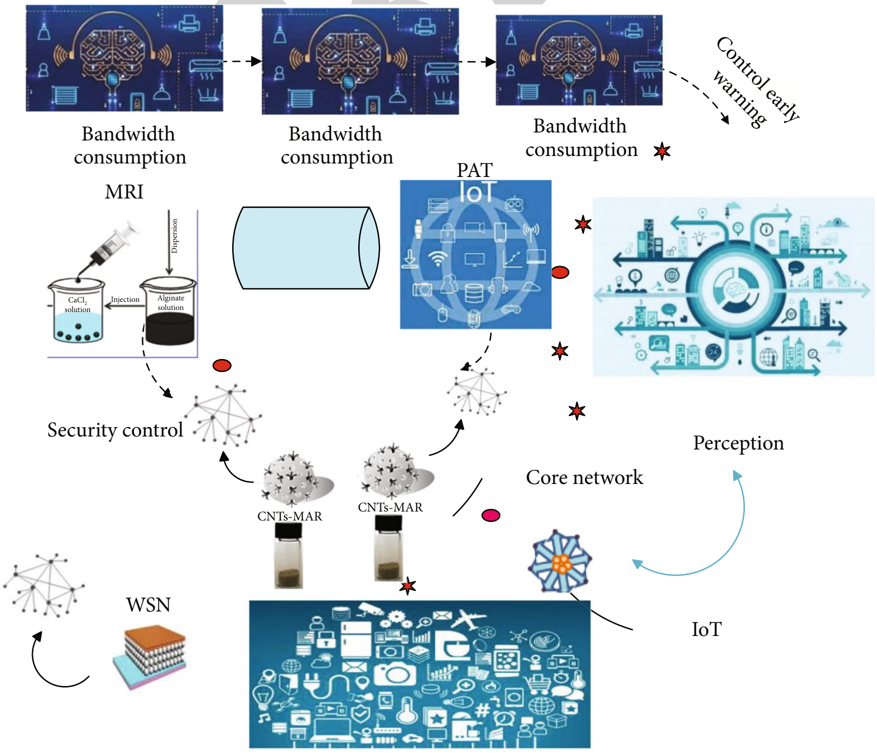

Figure 3: Security control WSN application scenarios.

```
For()
{if(the node is active) {
    If (node response time RT E normal response time range){
    Forward and process packets:
    (Node response time RT exceeds closed value)
    Detect whether the node is under malicious attack;
    If (node is maliciously attacked){
        Reassessing the alert situation;
        Multi-level early warning;
        Take defensive measures; }
    else{
    Forwarding and processing packets; }
}wait(t);
```

Algorithm 1: Security control model of network news dissemination based on bandwidth consumption attack on the Internet of Things

prompts according to the different degrees of attack. The influence coefficient is

$$\begin{aligned} P &= \frac{P + P^0}{P - P^0}, \\ \chi &= \frac{1 + \chi^0}{1 - \chi}, \\ \beta &= \frac{1 + C + H}{Q + C + H}, \\ &\begin{cases} \forall - \gamma P - \beta P - \chi = 0, \\ \gamma E - \beta E - \chi = 0. \end{cases} \end{aligned} \tag{1}$$

According to the above thoughts, warning prompt illustrates the node RT (response time) but may not be getting due to the causes of the node itself, but in the process of forwarding the path of the packet, when the target node appears unusual. It is necessary to check the nodes in the forwarding process from small to large in accordance with the forwarding level of nodes, so as to avoid the error of normal nodes and improve the accuracy of detection.

In addition, based on the response time of the attack more bandwidth consumption level detection of the early warning algorithm, in addition to the attack of detected early warning, severity will against network attacks take different defensive measures, and here are based on the response time of the attack more bandwidth consumption level detection warning algorithm the main logic description as shown in Algorithm 1:

The probability distribution of many random variables in production and scientific experiments can be approximately described by normal distribution, whom the central limit theorem from theory of normal distribution condition: if decided to the results of a random variable is the sum of a large number of small, independent random factors, single function and each factor that are relatively uniform are small, there is not a factor that can serve as the leading role, and overriding the random variables is generally similar to normal distribution. From a statistical point of view, the errors of various measurements are generally normally distributed. Therefore, it is considered that the results of multiple measurements of RTH should also follow normal distribution, and the normal distribution curve of RTH is shown in Figure 4.

3.3. Network Personal Information Security Control Technology and Its Characteristics

3.3.1. Biometric Identification Technology. Biological identification technology is through the computer and biological optics, acoustics, biological sensors, and biological principles of statistics and other high-tech means of closely combined, use human inherent physiological features, such as fingerprint, face, and iris, and the psychological characteristics of behavior, such as handwriting, voice, and gait, characteristics to effective identification and appraisal of personal identity. Because the biometric fingerprint identification of human body has a variety of nonreplicable biological characteristics, the security factor of this fingerprint identification technology has a great improvement and enhancement compared with the traditional biological identity authentication fingerprint identification mechanism. The identification features of retinal biological fingerprint applied to human body mainly include fingerprint, voice, aperture, retina, palmprint, and skeleton. Among them, retinal fingerprint has attracted much attention in the academic world due to its incomparable characteristics such as uniqueness, stability, and reproduction. In addition to the technology of retinal fingerprint recognition, the application and research of retinal fingerprint recognition technology and advanced signature fingerprint recognition technology have also made remarkable progress and achievements in recent years.

3.3.2. Network Security Vulnerability Scanning Technology. Network security vulnerability detection and safety risk assessment technology, because of its characteristic, can accurately predict the network main body possibility of various user network attacks, and specifically against emerging or over the safety of network attack behavior and possible risk consequences, and in recent years, by the network security technology attaches great importance to the industry. The security technology can help administrators identify and test the monitoring system, analyze the possible factors and indicators of the system resources being attacked by hackers, understand the security vulnerabilities of the network monitoring system, and evaluate all possible security risks. Network security vulnerability scanning technology, network firewall, intrusion system, and detection network monitoring system cooperate with each other, which can effectively protect and improve the quality and security of the whole network. By scanning the security vulnerabilities of the whole network, network administrators can timely understand the security settings of the whole network, the operation of the system, and the application services, timely discover the network security vulnerabilities, and objectively evaluate the risk and level of the whole network. Therefore, the network administrator can usually timely correct and find the network security loopholes and various wrong security settings in the process of system operation according to the network

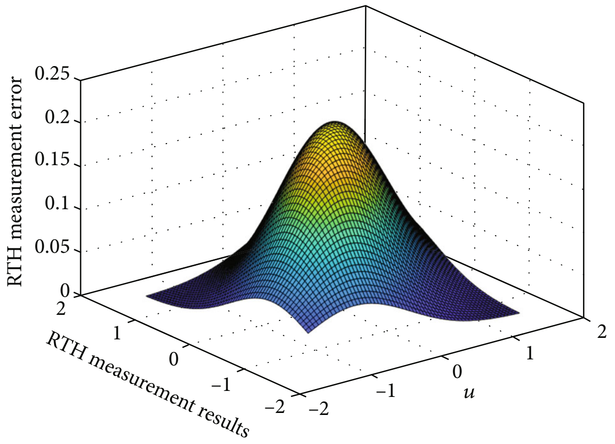

Figure 4: Normal distribution curve of RTH.

scanning status and results and guard against the system before the network is attacked by hackers. When the cluster gateway is determined, the remaining M-N nodes converge to the nearest gateway:

$$\begin{aligned} P_{ip} &= L_{ip} + (1-\chi)P_J, \\ P_{ip} &= L_{ip} + L(1-\chi)p. \end{aligned} \tag{2}$$

The certification interval is

$$\begin{aligned} T_P &= \min\left(p_0, \frac{y}{p_o}\right), \\ E(t) &= \int_0^t \frac{1}{1-p}\sqrt{\frac{\chi^2-p^2}{p_0}}dt. \end{aligned} \tag{3}$$

3.3.3. Detection Process of Abnormal Permission Configuration

Step 1. Clustering: clustering UPA to obtain similar user sets.

Step 2. Preprocessing of clustering results: before detecting abnormal permission configuration, the clustering results should be preprocessed first. For each class cluster, its characteristic pattern vector is constructed. For the elements in the feature pattern vector, if the column vector elements of the corresponding position in the class are all 1, then the position in the feature vector is set to 1, and all other positions are set to 0.

Step 3. Exception privilege configuration rule matching: in this stage, the exception privilege configuration candidate set is screened according to the preset exception privilege configuration mining rules, and the specific rules are as follows.

Rule 1. If a permission is granted only to users in a class, and the percentage of users granted the permission in the class is less than the threshold, mark this configuration as a correct configuration.

Table 1: Introduction of experimental data sets.

Data sets	Number of users	Access number
Healthcare	45	47
University	495	54
Emea	34	3146
Firewall 1	362	1427
Firewa112	324	1169

Rule 2. If a privilege is granted to users in more than one class, and if the proportion of users granted the privilege in the current class is less than the threshold value, then the intersection of the characteristic pattern vectors of the other classes contains the privilege, except this class.

Rule 3. If the proportion of users in a class that has not been granted a certain privilege to all users in the class is less than the threshold value, such configuration is defined as negative exception privilege configuration, these privilege configurations are added to the exception privilege configuration candidate set, and the corresponding position is set as t in the privilege configuration matrix.

Step 4. Cross clustering: after clustering according to the user's one permission matrix and mining the abnormal permission configuration, the row and column of the matrix are exchanged to obtain the transpose matrix of the matrix. Then, cross clustering is carried out according to the clustering algorithm proposed in this chapter. After the clustering results are obtained, the exception permission configuration candidate set is constructed according to the rules mentioned in Step 3.

Step 5. Exception privilege configuration decision: according to the above steps, two candidate sets of exception privilege configuration can be obtained, and the intersection operation of the two sets can be performed to obtain the common set. Define the elements in this common collection as the final exception permission configuration, and update the corresponding elements according to the appropriate modification principles.

Step 6. After dealing with all the clustering results, be able to get a new user access matrix, then the matrix as abnormal access configuration mining framework proposed in this chapter the input and iteration, until no abnormal access configuration is detected or cross the abnormal access configuration of the clustering algorithm to stop the candidate set intersection is empty.

4. Experimental Simulation

Firstly, the data set and evaluation method used in the experiment are introduced. Then, several groups of experiments are designed to compare and analyze the performance of the algorithm in this chapter from different perspectives. The data sets are shown in Table 1.

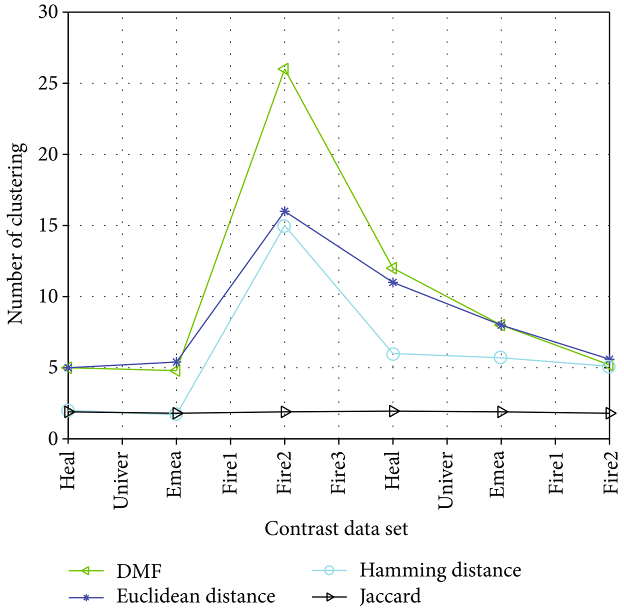

Figure 5: Comparison of the number of clusters.

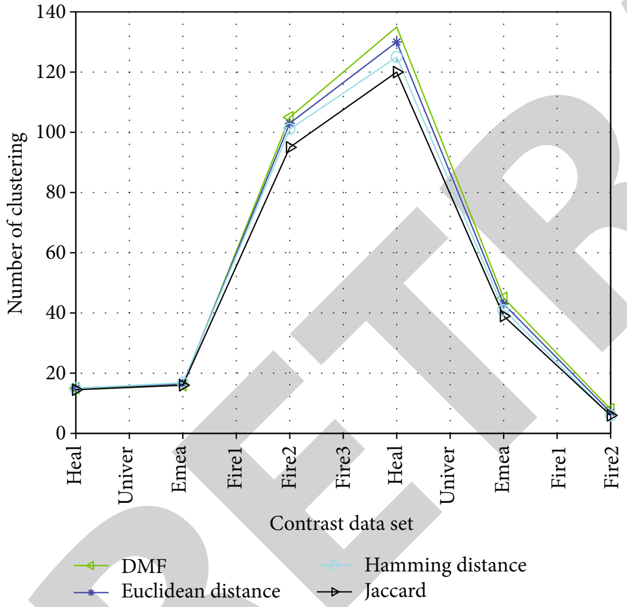

Figure 6: Comparison diagram of the number of generated roles.

In order to verify the effectiveness of DMF mentioned in this chapter, it was compared with Euclidean distance, Hamming distance, and Jaccard distance. As shown in Figure 5, compared with other distance functions, the DMF proposed in this chapter generates more clusters and can be used to distinguish users more effectively. At the same time, as shown in Figure 6, although the clustering algorithm proposed in this chapter increases the number of clustering, the number of roles finally generated does not increase significantly. This indicates that the clustering results under the traditional method are not accurate enough, and multiple roles may be discovered in a single class.

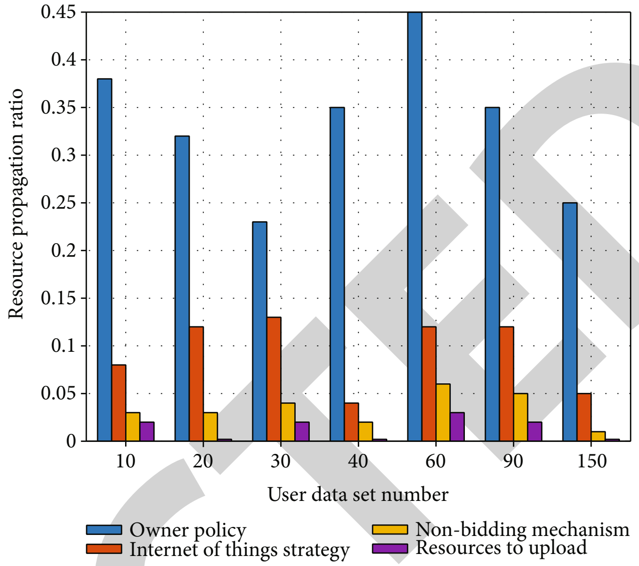

Figure 7: Comparison diagram of the proportion of network news communication resources under the environment of the Internet of Things.

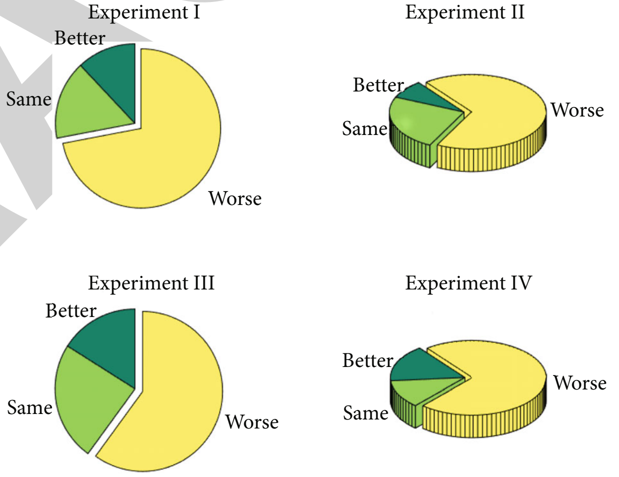

Figure 8: User satisfaction analysis diagram of security control.

As shown in Figure 7, this chapter takes some compensation measures. While increasing the proportion of resource transmission, it does not increase the loss caused by privacy leakage. However, the traditional nonbidding scheme requires users to voluntarily give up part of their privacy, which will still cause privacy loss while increasing the proportion of resource transmission.

In order to prove the universality of the scheme proposed in this chapter, we analyzed the data of all participants, presented the calculated results to participants, and collected their feedback. As shown in Figure 8, about 88% of participants believe that the strength of user relationships calculated by the scheme in this chapter can more accurately reflect their real relationships. According to the above conclusions, compared with the traditional scheme based on simple statistics, the calculation scheme of user relationship strength

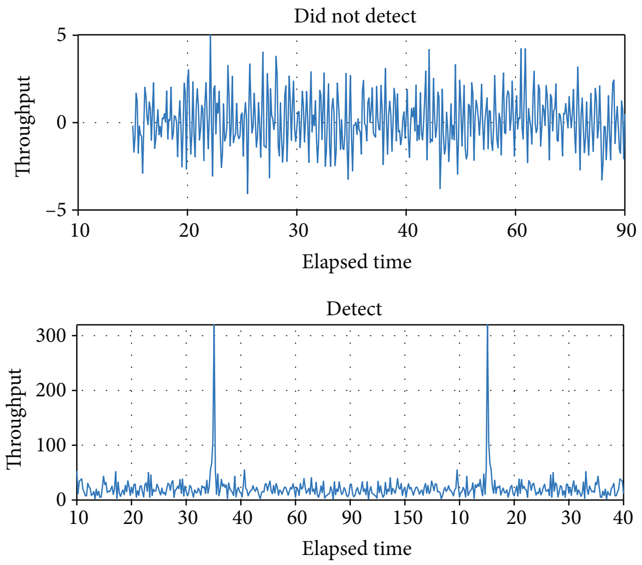

Figure 9: Throughput of the guard module without deep packet detection.

based on communication diversity proposed in this chapter can more accurately reflect the real relationship strength among different users.

In addition to the functional testing of the deep packet detection protection module, a stability test is also needed to compare the throughput and response time of the MATT direct transmission with the deep packet detection. In this experiment, the IxChariot throughput testing tool was used to test the performance of the Matt deep packet detection module. This testing tool supports the throughput and response time testing of various protocols and also supports the testing of customized application layer data. When the deep packet detection function is not added, the throughput of the protection module is shown in Figure 9.

5. Conclusion

By analyzing the characteristics of the Internet of Things, this paper analyzes the standard architecture of the industrial control of the Internet of Things and analyzes the interference factors in the Internet of Things environment from the perspective of the general control system model of the architecture and network environment and the security issues of the controlled system. The general control system model and the security model of the general control system under the environment of the Internet of Things are proposed. In view of transmission security, the security control model of Internet of Things news communication against bandwidth consumption attack is studied, and a detection algorithm of bandwidth consumption attack based on node response time is proposed. Under the guidance of the detection algorithm, a monitoring, analysis, and early warning model for bandwidth consumption attacks is constructed. Finally, through the analysis of simulation experiment and real user experiment results, it is proved that the proposed scheme can achieve dynamic and accurate resolution of coexisting policy conflicts. Security controls on the Internet of Things infrastructure will likely extend to the entire mobile network 10 times or even 100 times more than the Internet, which means the entire Internet of Things market of information security may also be expanded tens of times. The next step will be based on the coexistence strategy conflict resolution of communication diversity: the element types used in communication diversity calculation can be expanded to increase the universality of the scheme and improve the calculation accuracy of user diversity.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] S. Laghari and M. A. Niazi, "Modeling the internet of things, self-organizing and other complex adaptive communication networks: a cognitive agent-based computing approach," *PloS One*, vol. 11, no. 1, pp. e0146760–e0146772, 2016.

[2] V. Rohokale and R. Prasad, "Cyber security for Intelligent-World with internet of things and machine to machine communication," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 23–40, 2015.

[3] M. Durresi, A. Subashi, A. Durresi, L. Barolli, and K. Uchida, "Secure communication architecture for internet of things using smartphones and multi-access edge computing in environment monitoring," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 4, pp. 1631–1640, 2019.

[4] S. Jaloudi, "Communication protocols of an industrial internet of things environment: a comparative study," *Future Internet*, vol. 11, no. 3, pp. 66–86, 2019.

[5] Y. Jeong, "An emergence of network agenda-setting theory: a comparative analysis of networks of issue attributes between news media and online discussion forums," *Korean Journal of Journalism & Communication Studies*, vol. 59, no. 3, pp. 365–394, 2015.

[6] N. M. Martínez, J. J. Olivencia, I. Mac Fadden, and E. O. Olmedo, "Skills in the use of Technologies of Information and Communication of the teachers (2.0) under the scope of university studies," in *European innovations in education: research models and teaching applications*, E. L. Meneses, Ed., vol. 82, pp. 200–213, AFOE. Asociación para la Formación, el Ocio y el Empleo, 2017.

[7] I. Bladek and K. Krawiec, "Counterexample-driven genetic programming: heuristic program synthesis from formal specifications," *Evolutionary Computation*, vol. 26, no. 3, pp. 441–469, 2018.

[8] G. Chen, "Model innovation of network news communication based on interactive analysis," *Revista de la Facultad de Ingenieria*, vol. 32, no. 9, pp. 271–277, 2017.

[9] S. T. Campbell, "The dynamics of handcart as a means of informal transportation in support of logistics and tourism,"

Worldwide Hospitality and Tourism Themes, vol. 12, no. 1, pp. 48–55, 2020.

[10] M. Garau, E. Ghiani, and G. Celli, "Co-simulation of smart distribution network fault management and reconfiguration with LTE communication," *Energies*, vol. 11, no. 6, pp. 1332–1345, 2018.

[11] X. Wang, Y. Zhao, and H. Wu, "Research on the communication mode and strategy of hospital culture under the background of internet," *Boletin Tecnico/Technical Bulletin*, vol. 55, no. 14, pp. 583–588, 2017.

[12] R. Rahim, "Internet of things based driver exhaustion detection system using distributed sensor network," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 8, no. 4, pp. 12–16, 2020.

[13] C. Feng, Q. Chen, X. Cai et al., "Research on security problems and defense strategies of power communication networks," *IOP Conference Series: Materials Science and Engineering*, vol. 569, pp. 42047–42058, 2019.

[14] J. Kim, N. Heo, H. J. Jeon, and D. Jung, "Effects of simulation education on the communication competence, academic self-efficacy, and attitude about the elderly for nursing students: a learning approach based on an elderly-with-cognition-disorder scenario," *The Journal of Korean Academic Society of Nursing Education*, vol. 21, no. 1, pp. 54–64, 2015.

[15] A. Y. Zhou, "Society & the internet: how networks of information and communication are changing our lives," *Information Communication and Society*, vol. 21, no. 12, pp. 51–63, 2018.

[16] F. Y. Tseng and H. J. Yang, "Internet use and web communication networks, sources of social support, and forms of suicidal and nonsuicidal self-injury among adolescents: different patterns between genders," *Suicide and Life-Threatening Behavior*, vol. 45, no. 2, pp. 178–191, 2016.

[17] A. Noman and A. Ali, "Analysis and evaluation of survivability of various configured communication networks," *International Journal of Communication Systems*, vol. 11, no. 5, pp. 305–310, 2015.

[18] G. D. Seta, *Society and the Internet: How Networks of Information and Communication Are Changing Our Lives [Book Review]*, vol. 46, no. 2, 2015Communication Booknotes Quarterly, 2015.

[19] B. A. Vijayalakshmi, K. Ramkumar, and A. Aruna, "Up-and-coming Li-Fi technology under visible light communication to transfer the data among multiple users in train," *International Journal of Pure and Applied Mathematics*, vol. 119, no. 16, pp. 1587–1598, 2020.

[20] G. Stetz, L. Astl, and G. M. Verkhivker, "Exploring mechanisms of communication switching in the Hsp90-Cdc37 regulatory complexes with client kinases through allosteric coupling of phosphorylation sites: perturbation-based modeling and hierarchical community analysis of residue interaction networks," *Journal of Chemical Theory and Computation*, vol. 16, no. 7, pp. 4706–4725, 2020.

[21] L. Yan, Z. Wang, C. Liu, and Y. Wu, "On the determination and simulation of seawater freezing point temperature under high pressure," *Advances in Polar Science*, vol. 30, no. 4, pp. 38–45, 2019.

[22] J. N. Zavala, K. Ahrens, Y. N. Evans, and L. P. Richardson, "Adolescent obesity management: understanding the communication and support preferences of underserved youth," *Journal of Adolescent Health*, vol. 62, no. 2, pp. S121–S122, 2018.

[23] D. A. Aziz, "The importance of VLANs and trunk links in network communication areas," *International Journal of Scientific and Engineering Research*, vol. 9, no. 9, pp. 245–267, 2018.

[24] A. Al-Sammarraie, "The behavior of databases in maintaining the security of data transferred between two communication points," *International Journal of Civil Engineering and Technology*, vol. 9, no. 1, pp. 126–139, 2018.

[25] A. Lopez-Cazalilla, A. Ilinov, L. Bukonte et al., "Simulation of redistributive and erosive effects in a-Si under Ar^+ irradiation," *Nuclear Instruments and Methods in Physics Research Section B: Beam Interactions with Materials and Atoms*, vol. 414, pp. 133–140, 2018.

[26] D. Ding, Z. Wang, G. Wei, and F. E. Alsaadi, "Event-based security control for discrete-time stochastic systems," *IET Control Theory & Applications*, vol. 10, no. 15, pp. 1808–1815, 2016.

[27] G. Wen, W. Yu, X. Yu, and J. Lü, "Complex cyber-physical networks: from cybersecurity to security control," *Journal of Systems Science and Complexity*, vol. 30, no. 1, pp. 46–67, 2017.

[28] M. Shahpasand, M. Shajari, S. A. Hashemi Golpaygani, and H. Ghavamipoor, "A comprehensive security control selection model for inter-dependent organizational assets structure," *Information & Computer Security*, vol. 23, no. 2, pp. 218–242, 2015.

[29] W. Wang, Z. Gong, J. Ren, F. Xia, Z. Lv, and W. Wei, "Venue topic model–enhanced joint graph modelling for citation recommendation in scholarly big data," *ACM Transactions on Asian and Low-Resource Language Information Processing*, vol. 20, no. 1, pp. 1–15, 2021.

[30] R. Zhao, X. Wang, J. Xia, and L. Fan, "Deep reinforcement learning based mobile edge computing for intelligent internet of things," *Physical Communication*, vol. 43, p. 101184, 2020.

[31] W. Wei, Q. Ke, J. Nowak, M. Korytkowski, R. Scherer, and M. Woźniak, "Accurate and fast URL phishing detector: a convolutional neural network approach," *Computer Networks*, vol. 178, p. 107275, 2020.

[32] M. C. Chen, S. Q. Lu, and Q. L. Liu, "Uniqueness of weak solutions to a Keller-Segel-Navier-Stokes system," *Applied Mathematics Letters*, vol. 121, p. 107417, 2021.

[33] A. Zielonka, A. Sikora, M. Wozniak, W. Wei, Q. Ke, and Z. Bai, "Intelligent Internet of Things system for smart home optimal convection," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4308–4317, 2021.