Hindawi
Mathematical Problems in Engineering
Volume 2023, Article ID 9792076, 1 page
https://doi.org/10.1155/2023/9792076

Retraction

Retracted: Simulation of Dynamic User Network Connection Anti-Interference and Security Authentication Method Based on Ubiquitous Internet of Things

Mathematical Problems in Engineering

Received 18 July 2023; Accepted 18 July 2023; Published 19 July 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This article has been retracted by Hindawi following an investigation undertaken by the publisher [1].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] M. Pan, S. Tian, J. Yuan, and S. Chen, "Simulation of Dynamic User Network Connection Anti-Interference and Security Authentication Method Based on Ubiquitous Internet of Things," *Mathematical Problems in Engineering*, vol. 2021, Article ID 5687208, 8 pages, 2021.

Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 5687208, 8 pages
https://doi.org/10.1155/2021/5687208

Research Article

Simulation of Dynamic User Network Connection Anti-Interference and Security Authentication Method Based on Ubiquitous Internet of Things

Mingming Pan,[1,2] Shiming Tian ,[1,2] Jindou Yuan,[1,2] and Songsong Chen[1,2]

[1]*China Electric Power Research Institute, Beijing 100192, China*
[2]*Beijing Key Laboratory of Demand Side Multi-Energy Carriers Optimization and Interaction Technique, Beijing 100192, China*

Correspondence should be addressed to Shiming Tian; lss033@ncepu.edu.cn

Received 7 April 2021; Revised 22 April 2021; Accepted 14 June 2021; Published 22 June 2021

Academic Editor: Sang-Bing Tsai

Ubiquitous Internet of Things includes criteria, applications, and technologies for providing standard data. The system can be used to establish a comprehensive data database to facilitate people to better analyze, organize, and use these data, so as to improve the reliability and sharing of data, to provide better services for users. The purpose of this study is to propose and establish a specific and reliable data exchange program to ensure the security of data exchange. Data security is to ensure the reliability of specific security exchange process. The emphasis of this study is the reliability analysis method and the verification method of exchange process behavior. Based on the analysis of all abnormal phenomena in the Internet of Things traffic, the basic characteristics of network traffic, the basic properties of network traffic, and the theory of multiterminal power communication network anti-interference model construction and noninterference model, the simulation experiment of anti-interference and security authentication method is carried out. The results show that, with the increase of the number of antennas, the false detection probability decreases from 10^{-1} to 10^{-4}, which can achieve better performance in the detection of active users. When network is used in applications, HTTP + SSL is the most widely used application for data authentication and security authentication. The market of anti-interference technology is developing rapidly. The complex annual growth rate almost doubled in the international market, and the market scale was significantly expanded, with an annual growth rate of about 50%.

1. Introduction

1.1. Background and Significance. In the process of data security exchange, the exchange process is vulnerable to attack. The invaders use various attack means to destroy, camouflage, or interfere with the exchange process, so that the exchange cannot be carried out normally. The access process will cause security threats such as information tampering, leakage, and unauthorized access. For example, Trojan horse attacks are used to bring sensitive information or virus files to the data that is allowed to be exchanged, or, through attack bases, Trojan horses are used to disguise themselves and establish exchange channels for illegal data exchange. It can change the normal exchange process directly and destroy the expected behavior, so that the sensitive information in the exchange data can be read. These behaviors will bring security risks, such as disclosing sensitive information and spreading malicious code. Therefore, the anti-interference and security authentication technology of dynamic user network connection is particularly important.

1.2. Related Work. The Internet of Things will require ubiquitous information sharing among interconnected things around the world, which cannot be achieved by existing systems. The current research focuses on information dissemination solutions, which can lead to single point of failure and unnecessary communication delay. To this end, Victor proposed the SENSEable things platform, which is a fully distributed, open-source architecture for applications based on the Internet of Things. This paper

introduces the main problems that must be solved by IOT platform and Victor's technical solutions to these problems and evaluates these problems. Victor also introduces the current progress and a series of demonstrations to show the wide range of applications supported by the platform. Finally, Victor shows how the platform will be used for our future research and potential spin-off companies [1].

The proliferation of service-based and cloud-based systems has led to a situation in which software is often provided as a service and as a commodity through an enterprise network or global network. This scenario supports the definition of business processes as composite services, which are implemented through static or runtime combinations of products from different vendors. Quickly and accurately evaluating the security attributes of services became a basic requirement at that time, and now it has become a part of the software development process. Anisetti shows how to handle the security attribute validation of composite services through test-based security authentication and build it to be effective and efficient in dynamic composition scenarios. Anisetti's method is based on the existing single chip service security authentication scheme and extends it to service composition. It actually authenticates the composite service, starting with the certificate granted to the component service [2].

Android provides a permission statement and an authentication mechanism to detect and report potential security threats to applications. Usually, applications are authenticated based on their declared permissions, but the declared permissions are usually coarse-grained or inconsistent with the permissions actually used in the program code. Pei proposes an Android application programming interface (API) level security authentication (ASCAA) based on cloud computing. The framework uses a systematic method to identify and analyze API level security threats. To authenticate an application, ASCAA checks all permission tags in its manifest and API calls extracted from its decompiled code based on a set of requirements dependent on security rules. In addition, the author also provides ASCAA security language to standardize the security rules and authentication process, which makes ASCAA universal and extensible.

1.3. Innovation. This study analyzes the security management requirements of modern high security applications and proposes some new ideas and methods, system architecture, and key function technologies in the aspects of material selection and network design by using new Internet of Things technology. On the basis of the traditional technology and algorithm, we improved and innovated and finally formed a relatively complete experimental design. A variety of algorithms are proposed to promote the development of the system and adapt to complex environmental changes. At the same time, it has the characteristics of high positioning accuracy and high processing efficiency, which can meet the needs of experiments, so as to check the error detection rate of these algorithms for user activity.

2. Based on Mathematical Model

2.1. Threat Model. The current intelligent terminal system stores a large number of user privacy and even confidential information, which makes intelligent terminal become the target of more and more malicious users, including side channel attack against intelligent terminal and malicious utilization of current control technology fault, which deserves special attention [3]. This research is based on the following threat models: (1) Aiming at the stage connection of intelligent terminal user identity control technology, the intruder observes or captures the process of user's ID card input (but cannot directly observe the content displayed on the smart terminal screen) and steals the stable configuration information between the user's finger moving path and the relevant virtual keyboard getting user authentication credentials [4]. (2) For the explicit identification technology of intelligent terminal users in the connection stage, the intruder should be able to communicate with the intelligent terminal naturally and steal the user ID card through the oil residue or heat residue information on the touch screen [5]. (3) For the user identification technology of intelligent terminal in the connection stage, the intruder can install malicious software on the intelligent terminal; the user terminal system secretly records sensor data, such as the built-in acceleration sensor and gyroscope, on the corresponding equipment input by the user; according to the recorded sensor data, it may steal from the identity and user identity certificate [6]. (4) For the current intelligent terminal, there are certain defects in most of the user ID technology only after the user connects to the system before authentication. The intruder can naturally contact the intelligent terminal in the unlocking mode (such as leaving the unlocked mobile phone in the meeting room, classroom, and other occasions) or obtain the ability to interact with the intelligent terminal system through phishing attack. It can access the user's privacy and confidential information stored in the intelligent terminal [7].

2.2. Anti-Interference Model. The formal analysis of the security characteristics of data exchange by using strategic information flow can make us clearly understand the flow direction of information in the process of data exchange and observe the actual behavior of data exchange from another perspective independent of operation [8, 9]. By analyzing the information flow, we can verify whether the dynamic data exchange process can meet the security characteristics expressed by the given policy [10]. There are a lot of researches on information flow analysis, and antijamming is one of the most important research results. The anti-interference model can establish the system security policy model from the operation and operation results, instead of simply relying on the check of reading and recording functions to estimate the information flow. Compared with other information flow strategies, it can better reflect the dynamic implementation process of the system and the ability of different systems to communicate. In the exchange process, it can interact with each other and

detect the existence of hidden channels to avoid information leakage through hidden channels. Therefore, using an anti-interference model to analyze the reliability of exchange, process behavior has obvious advantages [11].

The concept of anti-interference is one of the main methods to determine or express the causal relationship between different security departments. It is also the theoretical basis for the standardization and analysis of security policies. The early research on anti-interference model is mainly applied to multilevel security system, dealing with deterministic system and information flow strategy with partial order relation. In short, this is the domain policy of H and l security departments [12]. This strategy is a transitional strategy, and many definitions of antijamming are based on these limitations. The anti-interference transfer strategy successfully provides the basis for multilevel security policy (MLS) and provides an official proof method [13].

Although the traditional anti-interference models successfully solve the multilevel security policy problem, some practical security problems are beyond the official description of the original definition, and these models have great limitations in practical application [14]. For example, MLS-based battle command systems only allow low-level to high-level domains, so when existing reports reach the highest level, they will not disclose information due to Trojan horse attacks. However, there is a major problem when a superior must publish business data to coordinate and manage the overall function. The system should allow limited information to flow from high-level domain to low-level domain [15]. Only through reliable control departments (e.g., degradation processing, decryption processing or encryption equipment), it cannot do that directly from the high-level domain to the low-level domain. Therefore, a nontransitive information flow strategy is most needed in the real world [16].

2.3. Dynamic User Network Connection. Taking a typical NOMA system with base station and user k as an example, it is assumed that the base station and each user are equipped with an antenna. After coding and channel configuration, active user K sends symbol xk from complex constellation set X, and XK transmits symbols to form SK distribution sequence with length J. Now we will focus on the case of $J < n$; that is, the number of users in the system is greater than the length of propagation sequence [17]. In this system, the signal from the active user will be converted and then transmitted by the k-rectangle OFDM payer [18]. The signal received from the base station can be expressed as.

$$y_n = \sum_{k=1}^{N} g_{nk} s_{nk} x_k + v_n, \quad n = 1, 2, \ldots, N. \tag{1}$$

Among them, s_{nk} is the nth component of SK dispersion sequence, VN is Gaussian noise in subcarriers, the mean value is zero, and the variance is σ^2. g_{nk} is the revenue of channel user k in the nth subcarrier. All subcarriers are the same and are distributed independently. Considering the Rayleigh fading channel in the algorithm, this clock channel model has been widely implemented [19]. The received signals on all subcarriers are combined, and then the received signal vector is $y = [y1, y2, \ldots yN]$, which can be expressed as.

$$y = Hx + v. \tag{2}$$

When $x = [y_1, y_2, \ldots y_N]$ is the channel equivalent matrix with the size of $n \times K$, the elements in the nth row and K column are equal to gnksnk, while the noise vector $v = [v_1, v_2, \ldots, v_N]T$ follows the CN $(0,\sigma^2 \mathrm{IN})$ distribution [20].

2.4. Anti-Interference Model Construction of Multiterminal Power Communication Network. On the basis of the above power communication network channel separation, the multiterminal network anti-interference model is established. The application of artificial intelligence technology in the ubiquitous Internet of Things creates communication connection and rapid networking and real-time perception and processing of information in power communication network [21]. Firstly, the multiterminal signal model is established, and the relationship between signal frequency and signal transmission rate is analyzed:

$$y = y_n \frac{v\beta}{Vm} \cos \overline{\omega}, \tag{3}$$

where y_n is the change in the transmission frequency detected by the receiver of a multiterminal network; V is the signal transmission speed; β is the transmission frequency of multiterminal power communication network; V is the transmission power of power grid; cos ω is the angle between power distribution direction and electromagnetic wave incidence; and y is the signal frequency of power communication network [22, 23]. According to the above signal model, the linear signal in the power communication network is time-varying. Assuming that the monitoring error in the power communication network is $e_x = x\text{-}x_n$, the impulse response of the channel is a random process, which needs to be satisfied.

$$K(a_k) = E\left\{\frac{w}{y_n}, e_x + a\right\}, \tag{4}$$

where W is the state information of power communication network; a is the reference signal; and E {·} is the impulse response of communication signal. On this basis, the scattering function of power communication network signal is defined as

$$s(j) = \frac{F\{d(c,t)\}}{K(a_k)}, \tag{5}$$

where j is the scattering signal of power communication network; $F\{\cdot\}$ is the total data transmission in the communication network; and $D(C, t)$ is the channel function of power communication network. On the basis of the above calculation, the state equation of multiterminal power communication network after interference suppression is obtained:

$$R(x) = b\sum_{i=0}^{b} hx\left(\frac{t}{2B} - zr\right), \quad (6)$$

Here, H is the communication signal bandwidth of multiterminal power communication network; B is the sampling interval; and R is the number of power terminals. When the two state signals in the multiterminal power communication network are the same, the correlation peak value is the largest, which can be sent by the correlation monitor. However, when there are single frequency, narrowband, multipath, and multiple access interference, the signal power needs to be decoupled to filter other signals [24]. Through the above definition, the anti-interference model of multiterminal power communication network based on ubiquitous Internet of Things is obtained.

3. User Network Anomaly Detection

3.1. Experimental Setup. In order to analyze the abnormal traffic of all network users, this paper defines the network traffic sequence according to the basic characteristics of network traffic and describes the external characteristics of network traffic comprehensively. According to the network traffic order, the deep learning method is used to self-study the anomaly detection features, and the abnormal traffic is classified, detected and classified. Since the method proposed in this study is only based on the external characteristics of the network flow and does not analyze the content of the message, it can be applied to anomaly detection of encrypted traffic.

3.2. Experimental Process. The experiment outputs the basic characteristics of network traffic, in which IP address is the address of remote terminal, and traffic type is specific type of network mobile protocol, such as TCP and UDP. Message length is the size of a single message. The time of receiving information refers to the time between additional information. The flow of information is divided into personnel flow and outflow. The basic characteristics of the output network traffic are prepared in advance to receive the final network flow order vector.

Firstly, the time period characteristics of traffic packets are obtained. Traffic can be regarded as two time lines: a sequence of incoming packets of different sizes with time marks and a sequence of outgoing packets. The number of bytes transmitted in each time unit of these two time series in a specified time period is calculated. As a result, each data stream is converted to a distribution of the same size. Then the frequency sector characteristics of traffic packets are obtained. For the initial message length, message receiving time and other data, the time sequence information is transformed into frequency domain information by Fourier transform, and the former value is selected as the network traffic sorting ability. Finally, normalization is used to make each presence (such as message duration and time period) of the same order of magnitude in the feature. The vector formed by the final calculation result is the network flow sequence.

Network flow order vector can be used as input data to detect abnormal access to terminals. In order to detect the anomaly in the business process of Internet of Things terminal, we further understand the anomaly detection features from the network flow sequence. The steps to use the self-learning feature algorithm are as follows. Firstly, the algorithm model is selected and a self-coding network model with two hidden layers is used. The whole self-coding network model includes one input layer, two hidden input layers, one hidden output layer, and one output layer. Each level is associated with a fully connected method. Then the parameters of the model are specified, and the weight W of the network connection is determined by the adaptive torque estimation algorithm, and the anomaly detection features are derived. After the attributes are derived, the carrier outlet of the second layer of the self-coding model is taken as the carrier.

3.3. Abnormal Detection Method. After understanding the characteristics of anomaly detection, the combination of automatic white list matching algorithm and single class support vector machine algorithm should be used to detect abnormal network movement. For the characteristics of IP address and traffic type, IP address or access type that is not in the scope of the whitelist is defined as abnormal traffic directly, and list matching method should be used. If the IP address and access type are normal, the known anomaly detection function is used as the input, and the single class support vector machine algorithm is used to determine whether it is abnormal. In the training stage, the goal of single class SVM learning is to construct a discrete function which can classify data samples as accurately as possible. Therefore, single class support vector machines should first correspond to the entry points of high-dimensional space through core operations and then separate them as far as possible from their origin in dimensional space. In the detection phase, only the discrete function obtained in the training phase is needed to identify the flow detection characteristics. If the calculation result is 1, the flow to be measured is considered as abnormal flow; otherwise, it is normal flow.

4. Security Authentication Simulation

4.1. Software Simulation. By simulating the authentication process of the new protocol by software, the communication between the read-write server and the supporting server is generally considered to be secure, so they can be considered as a whole. In other words, software simulation only needs to verify the bidirectional identification process between reader and tag. The software simulation adopts the simulation new protocol, and the data storage should adopt the protocol and database. Four tables are created in the database, including illegal tags, illegal readers, legal tags, and legal readers. Among them, serial number 1–5 is illegal label, and serial number 5–10 is legal label. Each table in the database contains field names, bit data, data types, and specific concepts. Label and reader are shown in Tables 1 and 2,

Table 1: The label table contains information.

Field	Data bits	Data type	Specific meaning
Tag number	36	Int	Tag number
PID	64	Int	Katakana
ID	64	Int	Tag id
K1	64	Int	Secret key
K2	64	Int	Secret key
K3	64	Int	Secret key

Table 2: The reader table contains information.

Field	Data bits	Data type	Specific meaning
PID	64	Int	Tag number
ID	64	Int	Katakana
K1	64	Int	Tag id
K2	64	Int	Secret key
K3	64	Int	Secret key
G1	64	Int	Secret key
G2	64	Int	Secret key

respectively. Among them, the illegal tag key is incompatible with the public read-write key and does not include the key set created by PUF unit, as shown in Tables 1 and 2.

Firstly, two subroutines are written in Java to represent the reader and tag, and then four functional units are created, which are communication function unit, call database function unit, encryption function unit, and protocol verification function unit. The functional communication unit is used for communication and data transmission between two subprograms (reader subroutine and label subroutine). The communication unit uses socket technology to ensure the communication between two subprograms. The function data unit should call two subroutines to call and update the database data. The function encryption unit is mainly responsible for processing the encryption and decryption key of the call data, mainly completes some bit processing operations, and forms a part of the protocol. The PUF unit on the label is a physical circuit. Its basic idea is that when a binary code is inserted into the PUF unit, the latter unit can create a unique output as the key entry and exit, and there is no way to retreat. Therefore, the functional software analog encryption unit contains an irreversible key generation algorithm to replace the PUF material circuit. The verification unit is mainly responsible for the information transmitted according to the protocol to determine whether the reader and tag are legal.

4.2. Dynamic User Activity. Orthogonal matching pursuit (OMP) algorithm is a common compressed sensing recovery algorithm. Compared with curve optimization algorithm, OMP algorithm ensures the accuracy of signal recovery with lower algorithm complexity. From the perspective of matrix association, the synchronous SOMP algorithm, the normalized focus algorithm based on MMV model, and the correlation orthogonal search algorithm (OMP) are compared. When the number of active users N_a and the number of antennas $M = 128$, $M = 256$, the active user detection efficiency of OMP-KR algorithm changes. It can be seen from the figure that when the number of active users is $N_a \leq 10$, the error detection probability of OMP-KR algorithm is zero. It can detect fully active users and inactive users, while SOMP and m-focus algorithms have errors. Look at the situation. With the increasing number of active users Na, the probability of error detection in OMP-KR, SOMP, m-focus algorithm also increases gradually. However, it can be seen from the figure that OMP-KR algorithm is obviously superior to the other two algorithms. Even in the case of a large number of active users, OMP-KR algorithm can still guarantee low false detection probability, while in the other two cases, the error classification probability of the algorithm is close to 1. This shows that OMP-KR algorithm can support more active users than SOMP and m-focus algorithm. At the same time, when the number of antennas changes from $M = 128$ to $M = 256$, the yield of OMP-KR algorithm is very considerable. From the shape, OMP-KR algorithm is wrong when the number of active users $N_a = 20$. The detection probability decreases from 10^{-1} to 10^{-4}, which shows that OMP-KR algorithm can obtain better active user detection performance with the increase of the number of antennas, as shown in Figure 1.

When the number of active users is $N_a = 5$, the detection efficiency of OMP-KR algorithm varies with the change of noise, and the number of antennas is $m = 128$ and $M = 256$. Considering the number of antennas $M = 256$, the OMP-KR algorithm proposed in this study has zero detection error probability and can detect fully active users and inactive users. The error detection probability of the other two algorithms is not zero, in which the SOMP error detection probability is 10–1, and the m-focus error detection probability is 1; that is, the m-focus algorithm is 10log10 (1/SZ2) = 0 dB, which is completely invalid and cannot be identified as an active user.

4.3. Verification Vulnerability. Because apps with validation vulnerabilities are not malicious applications, they are still popular in the large Android software market. This study shows that the sensitivity test is not aimed at large-scale app dataset detection. The main research goal is to protect the real-time detection and security of mobile Internet for the application of users on mobile devices. One is to use interactive environment analysis unit to dismantle 500 sets of application programs, analyze the code source code, and use static detection method to control the use of application network. The statistical test shows the statistical results using 500 application networks, as shown in Figure 2.

HTTP + SSL authentication function is widely used in current applications, accounting for 38%. Among the 500 applications, 190 applications use HTTP + SSL for data verification and security, 155 applications use HTTP for data communication, 75 applications use receivers for data exchange, and 40 applications do not use network data. Then, using SSL to dynamically detect and analyze 40 applications determines whether there are security verification vulnerabilities in these applications. Combined with automatic testing and dynamic creation of test certificates, it is found

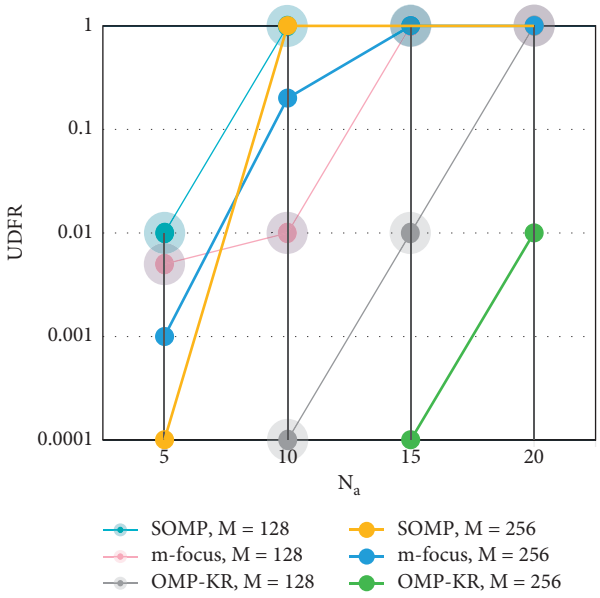

Figure 1: The influence of active user detection performance.

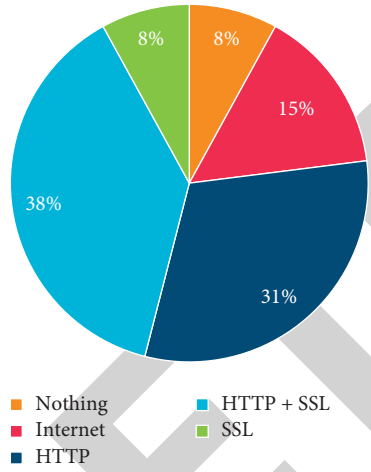

Figure 2: Statistical distribution of network usage in applications.

that 13 of these 40 applications have SSL verification leak holes through dynamic testing.

4.4. Safety Certification Method. In order to count the delay of E-SSL network in the process of security detection and security service, it is necessary to record the average time of regular visit, access SSL by security detection and security application, and compare security detection and security detection network with contract access. Because SSL has the function of reusing operation cycle, continuous access will not create a complete SSL handshake process in the specified time period. Therefore, intermittent access mechanism is used to calculate the average time. In this study, the test application and E-SSL client were used to make 20 intermittent visits to the E-SSL server, and the time of each visit was recorded, as shown in Figure 3.

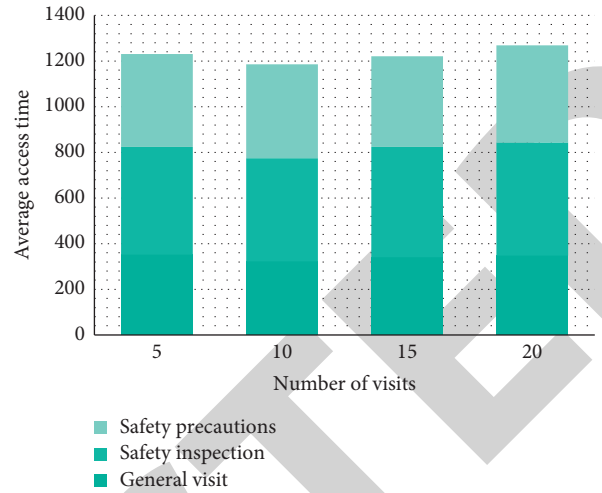

Figure 3: Visit time.

In order to view the statistical results more conveniently, we choose to calculate the average time of different visit time and observe the change trend of the visit time. The first 5 times, 10 times, 15 times, and 20 times were selected as observation points. Generally speaking, HTTP time is equivalent to TCP handshake time, and HTTPS time is equivalent to TCP handshake time plus SSL handshake time. SSL handshake time is relatively longer than TCP handshake time. Through the observation and analysis of the experimental data, this study draws two conclusions: (1) the security detection function takes longer than normal access, because the security detection service performs more SSL handshake process than normal access. (2) Compared with the conventional access, the time spent by the security protection service is almost the same, because the security countermeasure protection service only carries out the port switching and forwarding process. In order to ensure the security of user's privacy, the network delay is within the tolerable range without affecting the user's online experience.

4.5. Delay and Availability before and after Anti-Interference Technology. In terms of the development status of anti-interference technology, among the top 10000 websites in Alexa's global websites, the market share of the United States is far ahead. For example, with the highly distributed content delivery system deployed in more than 100 countries around the world, covering more than 2000 networks and more than 302 thousand servers and providing more than 80 terabits of web traffic per second every day, it provides nearly 3.5 trillion Internet interactions every day.

As shown in Figure 4, the use of anti-interference technology has a great effect. The utilization rate of anti-interference technology for large-scale websites is higher than that for small- and medium-sized websites. Therefore, in order to reduce the operating costs of enterprises, improve the flexibility of enterprises, and improve the service quality of companies, many large companies have begun to establish their own anti-interference systems. On the basis of meeting

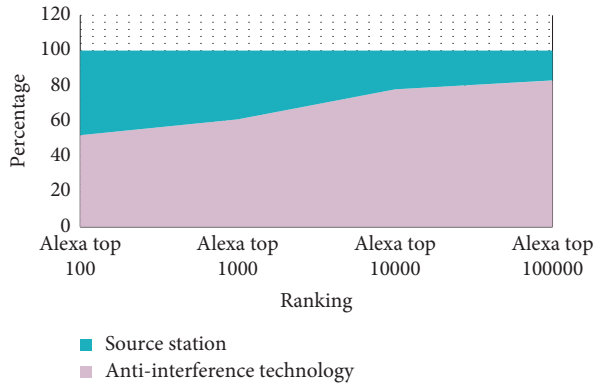

Figure 4: Schematic diagram of comparison between before and after delay and availability.

their own needs, it provides anti-interference external business technical services for the company to expand new business areas. In terms of domestic development, according to the statistics of China Institute of Information and Communications, China's market for anti-interference in the technical service industry has developed rapidly, with the compound annual growth rate almost doubled, and the international market scale has expanded significantly, with an annual growth rate of 50%.

5. Conclusions

Generally speaking, with the continuous development and maturity of antijamming technology, the service it can provide is more and more comprehensive and intelligent, which has attracted the attention of many scholars at home and abroad and is committed to the research and optimization of anti-interference technology. For example, in order to optimize the temporary storage and distribution of content in order to provide services to users, on the one hand, it reduces the user access delay, and on the other hand, it improves the access rate performance of the temporary storage for user access requests; the system has been designed in theory, applied and tested, and the results have achieved the expected design goals. The stability of network management technology, the applicability of location algorithm, and the low power consumption and effectiveness of security algorithm all have better performance than traditional algorithms.

The simulation results show that the system can meet the functional and technical requirements of the system. Compared with the traditional MMV algorithm: SOMP algorithm and m-focus algorithm, OMP-KR can support more active user detection. When the number of active users is the same, OMP-KR algorithm is better than the traditional MMV algorithm. With the increase of the number of antennas, OMP-KR algorithm may obtain more benefits than the traditional MMV algorithm.

Aiming at the problem of poor anti-interference performance of traditional multiterminal network anti-interference methods, the ubiquitous system Internet of Things is based on the ubiquitous Internet of Things, and an anti-interference method of multiterminal communication network is designed. This design realizes the anti-interference of multiterminal power communication network from the transmission channel segment of power communication network and the anti-interference of model multiterminal power terminal communication network. The experimental results show that the design method has good anti-interference performance. In conclusion, the antigrid interference method designed in this paper improves the performance of antigrid interference, has good implementation value for the management of power communication network, and can promote the development of power communication network.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] V. Kardeby, S. Forsström, and P. Österberg, "Fully distributed ubiquitous information sharing on a global scale for the internet-of-things," *International Journal on Advances in Telecommunications*, vol. 7, no. 3, pp. 69–81, 2015.

[2] M. Anisetti, C. Ardagna, E. Damiani et al., "Test-based security certification of composite services," *ACM Transactions on the Web*, vol. 13, no. 1, pp. 69–111, 2019.

[3] T. P. Hammerberg, "Anomaly detection," *Encyclopedia of Social Network Analysis and Mining*, vol. 83, no. 11, p. 78, 2018.

[4] D. B. Hess, E. Iacobucci, and A. Väiko, "Network connections and neighbourhood perception: using social media postings to capture attitudes among twitter users in Estonia," *Architecture and Urban Planning*, vol. 13, no. 1, pp. 67–78, 2017.

[5] J. E. Kurz and D. M. Chetkovich, "Understanding network connections connects genotype to epilepsy phenotype," *Epilepsy Currents*, vol. 17, no. 4, pp. 239-240, 2017.

[6] B. S. R. Farr-Wharton, K. Brown, R. Keast, and Y. Shymko, "Reducing creative labour precarity: beyond network connections," *Management Decision*, vol. 53, no. 4, pp. 857–875, 2015.

[7] A. A. Branitskiy, "Hierarchical hybridization of binary classifiers for detecting anomalous network connections," *SPII-RAS Proceedings*, vol. 3, no. 52, pp. 204–233, 2017.

[8] A. Sameh and A. Al-Masri, "Smartphones network connections power-aware multiple wireless interfaces," *Asian Journal of Information Technology*, vol. 18, no. 2, pp. 37–48, 2019.

[9] N. Zhao, J. Guo, F. R. Yu, M. Li, and V. C. M. Leung, "Antijamming schemes for interference-alignment-based wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1271–1283, 2017.

[10] Z. Hu, M. Xiong, H. Shang, and A. Deng, "Anti-interference measurement methods of the coupled transmission-line capacitance parameters based on the harmonic components," *IEEE Transactions on Power Delivery*, vol. 31, no. 6, pp. 2464–2472, 2016.

[11] L. N. Bao, R. B. Wu, D. Lu, and W. Y. Wang, "A novel adaptive anti-interference algorithm based on negative diagonal loading for spoofing and jamming in Global Navigation

Satellite System," *Journal of Communications Technology and Electronics*, vol. 61, no. 2, pp. 157–164, 2016.

[12] Y. Wang, L. Wu, and Y. Yang, "Security authentication method of terminal trusted access in smart grid," *International Journal of Security and Its Applications*, vol. 9, no. 7, pp. 337–346, 2015.

[13] X. Jiang, Y. Mei, and H. Yang, "Development and application of wireless data acquisition system of ground pressure in similar simulation experiment," *Coal Technology*, vol. 47, no. 2, pp. 56–60, 2016.

[14] W. Li, L. Lu, Z. Liu et al., "HIT-SEDAES: an integrated software environment for simulation experiment design, analysis and evaluation," *International Journal of Modeling Simulation & Entific Computing*, vol. 7, no. 3, pp. 1650027.1–1650027.22, 2016.

[15] G. Lee, J. W. Bae, N. Oh, J. H. Hong, and I. C. Moon, "Simulation experiment of disaster response organizational structures with alternative optimization techniques," *Social Science Computer Review*, vol. 33, no. 3, pp. 343–371, 2015.

[16] S. Wei, Z. Ma, B. Li et al., "Study on the monitoring method of three-dimensional stress with FBG in surrounding rock and the simulation experiment," *Caikuang Yu Anquan Gongcheng Xuebao/Journal of Mining and Safety Engineering*, vol. 32, no. 1, pp. 138–143, 2015.

[17] Q. Chen, F. Zhao, and Y. Wang, "Orthogonal simulation experiment for flow characteristics of ore in ore drawing and influencing factors in a single funnel under a flexible isolation layer," *JOM*, vol. 69, no. 12, pp. 1–7, 2017.

[18] K. K. Gu, W. J. Wang, J. Guo et al., "Tribological simulation experiment of interactions between rail and grinding stone," *Mocaxue Xuebao/Tribology*, vol. 35, no. 2, pp. 154–159, 2015.

[19] W. Yan, W. Xiang, S. C. Wong, X. Yan, Y. C. Li, and W. Hao, "Effects of hands-free cellular phone conversational cognitive tasks on driving stability based on driving simulation experiment," *Transportation Research Part F: Traffic Psychology and Behaviour*, vol. 58, pp. 264–281, 2018.

[20] C. Liu, F. Li, Z. Sun et al., "Electric simulation experiment procedure for predicting productivity of multi-stage fractured horizontal wells," *Oil & Gas Geology*, vol. 38, no. 2, pp. 385–390, 2017.

[21] Y. Cai, L. Shengdong, and L. Lu, "Water abundance of mine floor limestone by simulation experiment," *International Journal of Mining Science & Technology*, vol. 26, no. 03, pp. 130–135, 2016.

[22] X. Zhaohui, W. Yan, L. Jing et al., "Simulation experiment of the impact on the motion of the particle in dual-phrase distribution of gas & solid under strong electric field," *High Voltage Apparatus*, vol. 51, no. 7, pp. 171–176, 2015.

[23] D. B. Rawat, R. Alsabet, C. Bajracharya, and M. Song, "On the performance of cognitive internet-of-vehicles with unlicensed user-mobility and licensed user-activity," *Computer Networks*, vol. 137, no. 4, pp. 98–106, 2018.

[24] B. Wang, L. Dai, Y. Zhang, T. Mir, and J. Li, "Dynamic compressive sensing-based multi-user detection for uplink grant-free NOMA," *IEEE Communications Letters*, vol. 20, no. 11, pp. 2320–2323, 2016.