Hindawi
Complexity
Volume 2023, Article ID 9794650, 1 page
https://doi.org/10.1155/2023/9794650

Retraction

Retracted: Internet of Things Security Detection Technology Based on Grey Association Decision Algorithm

Complexity

Received 15 August 2023; Accepted 15 August 2023; Published 16 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This article has been retracted by Hindawi following an investigation undertaken by the publisher [1].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] J. Chang, X. Zuo, B. Hou, L. Shi, and G. Zhang, "Internet of Things Security Detection Technology Based on Grey Association Decision Algorithm," *Complexity*, vol. 2021, Article ID 7504806, 12 pages, 2021.

Hindawi
Complexity
Volume 2021, Article ID 7504806, 12 pages
https://doi.org/10.1155/2021/7504806

Research Article

Internet of Things Security Detection Technology Based on Grey Association Decision Algorithm

Jie Chang,[1] **Xiaojun Zuo**,[1] **Botao Hou**,[1] **Lipeng Shi**,[1] **and Guanghua Zhang**[2]

[1]*State Grid Hebei Electric Power Research Institute, Hebei Province, Shijiazhuang 050021, China*
[2]*School of Information Science and Engineering, Hebei University of Science and Technology, Shijiazhuang 050021, China*

Correspondence should be addressed to Jie Chang; dyy_changj@he.sgcc.com.cn

Received 28 April 2021; Revised 25 May 2021; Accepted 10 June 2021; Published 18 June 2021

Academic Editor: Zhihan Lv

This paper analyzes the current real-time monitoring system based on grey-related IoT security sensors for the detection of risk factors in the production environment of the Internet of Things and proposes a design plan for the Internet of Things environment monitoring based on the grey-related Internet of Things security sensor network, and according to the reliability guarantee mechanism of the system, a three-dimensional uniform IoT node deployment method suitable for IoT security monitoring is proposed. Based on the grey correlation analysis, it can provide a quantitative measurement analysis for the development and change state of a system, which is very suitable for the analysis of dynamic operating systems. As a real-time dynamic system of the Internet of Things, the use of grey correlation method to analyze its network security status has good operability and practical value. According to the multisource information processing technology, the monitoring data are preprocessed by dynamic limiting filtering, and then the data are fused at the data level with the optimal weighting algorithm. Through the use of grey correlation analysis to quantify the relative impact of cyberattacks on the network within a certain period of time, the quantitative assessment of the security environment and status of the entire network is realized. Finally, the characteristics of grey relational analysis and rough set theory attribute reduction are used to form the basis of grey correlation decision-level fusion algorithm, to achieve effective processing of the data of the Internet of Things security monitoring system.

1. Introduction

Real-time monitoring of the operating environment of the Internet of Things is one of the important means to prevent the occurrence of Internet of Things accidents and improve the safety management of the Internet of Things [1]. With the comprehensive advancement of the Internet of Things in all walks of life, security issues have become a key issue to be solved. Research has shown that the special geological conditions and harsh environment of the Internet of Things are very suitable for combining the grey-related Internet of Things security sensing technology [2]. At present, in China, many types of Internet of Things are still monitored by traditional wired methods [3]. The grey relational Internet of Things security sensor network technology is widely used in monitoring systems [4]. Therefore, most of the domestic Internet of Things is a wired monitoring system, and the technical approach is active FIRD combined with communication methods such as Ethernet [5]. In order to effectively respond to cyber threats, various research institutions and functional departments have strengthened their protection efforts [6], building a single-point defense system [7]. However, these defense tools often only focus on the partial information of cyber threats and timely and accurately detect threat behaviors and their internal associations, resulting in large deviations in detection results and formulating security strategies for network administrators [8].

Foreign Internet of Things security monitoring technology began to develop in the 1960s, there have been four generations of products today, and a new generation is basically every ten years [9]. It is a comprehensive automated IoT monitoring system that covers the entire process flow, is compatible with various monitoring technologies, and

realizes the automatic monitoring of the environmental parameters of the Internet of Things [10]. In the middle and late last century, a CMC-1 type associated decision-making monitoring system with 128 monitoring points was introduced to monitor environmental parameters [11]. With the advancement of science and technology and the advent of advanced instruments, many countries have developed many monitoring and control systems [12]. Kougianos et al. [13] are the first to propose the use of grey correlation sensor networks in the Internet of Things to realize worker tracking and positioning and environmental parameter monitoring. The application of domestic monitoring technology is relatively late [14]. In the early 1980s, the country introduced a batch of monitoring systems from France, Poland, Germany, the United States, and the United Kingdom [15]. At the same time, in the process of introduction, through digestion and absorption, combined with the actual situation of the national Internet of Things, we have successively developed the KJ70 Internet of Things safety monitoring system [16]. In recent years, comprehensive mine safety monitoring systems are based on Ethernet. Swan [17] has been widely used in the Internet of Things industry, but these systems still have insufficient scalability, low flexibility, and small coverage area. Therefore, in order to ensure the reliability of information transmission and increase the data transmission speed, reduce the blind area of safety monitoring [18]. The emergence of the grey-related IoT security sensor network (WSN) has brought new ideas to the IoT security monitoring system. Its unique advantages such as easy expansion, flexible placement, self-organization, and strong mobility can integrate the information of the realization system [19]. However, due to the particularity of the working environment of the grey-related IoT security sensor network, the existing research results cannot be directly applied [20]. Nesa et al. [21] and others referred to the research results of situational awareness in other fields and proposed a network security situational awareness model based on data fusion. Balamurugan et al. [22] applied data fusion technology to the network intrusion detection model to realize the network situation awareness system. Zhang et al. [23] and others designed a new fusion algorithm to improve the accuracy of situational awareness, through the threat detection and identification system to deal with complex events. Safaei Pour et al. [24] introduced an adaptive human-computer interaction fusion system to identify threats. At the same time, Lin et al. [25] designed an unknown threat detection method based on the concept of conflict in the environment, which effectively solved the problem of unknown threat identification frequently encountered in the multi-IoT security sensor automatic target recognition system and situation assessment. In recent years, with the research and development of network security situation assessment technology, data visualization technology has been regarded as a key technology in the network security situation assessment system, which has attracted the attention of domestic and foreign scholars and has achieved considerable development and application. Ma and Pang [26] realized Erbacher's IDS visualization system based on the logs collected by Hummer IDS and developed a network traffic sensing system based on NetFlow, using network traffic analysis tools to analyze the network connection relationships and traffic characteristics in the network in a visual way.

From the results of theoretical analysis and simulation, the node deployment method and reliability guarantee mechanism proposed in this paper have the characteristics of high coverage of the monitoring area, balanced energy consumption, flexibility, and scalability. On the basis of discussing the main security problems of the Internet of Things, this paper discusses the method of evaluating the security status of the Internet of Things based on the grey association algorithm and carries out a corresponding empirical analysis. In view of the above problems, the application of networked security sensor network technology in the field of security monitoring of the Internet of Things provides new ideas for safe production of the Internet of Things and has a significant effect on improving the topological reliability of the security monitoring of the Internet of Things. Through a more detailed discussion on the security issues of the Internet of Things, combined with the grey correlation algorithm, the method and steps of the Internet of Things security status assessment are proposed, and through empirical analysis, the specific process of the application of the grey correlation algorithm in the security status assessment of the Internet of Things is explained. It has a certain reference significance for the Internet of Things managers to ensure information security and manage the Internet of Things in practical applications.

2. Construction of IoT Security Detection Model Based on Grey Association Decision Algorithm

2.1. IoT Security Detection Level. The grey relational Internet of Things security sensor network technology is a new generation of network technology based on the fourth-generation grey relational communication technology and integrating traditional sensing, embedded computing, distributed information processing, and monitoring technologies [27–32]. Nodes are composed of IoT security sensor modules, processor modules, grey correlation communication modules, and energy supply modules [33–35]. According to their functions, they can be divided into four categories: node coordinator, router, enhanced end device node, and streamlined end device node. Network security status analysis usually includes several aspects such as the operation status of various network equipment at a certain time, network service status, and user behavior analysis and evaluation. The grey correlation IoT security sensor network measures the signals of the surrounding environment through the built-in IoT security sensors in the node, thereby detecting humidity, temperature, noise, soil composition, pressure, light intensity, size, speed, and direction of moving objects.

It mainly includes the physical layer, data link layer, network layer, transport layer, and application layer from Figure 1. In addition, the protocol stack also includes three

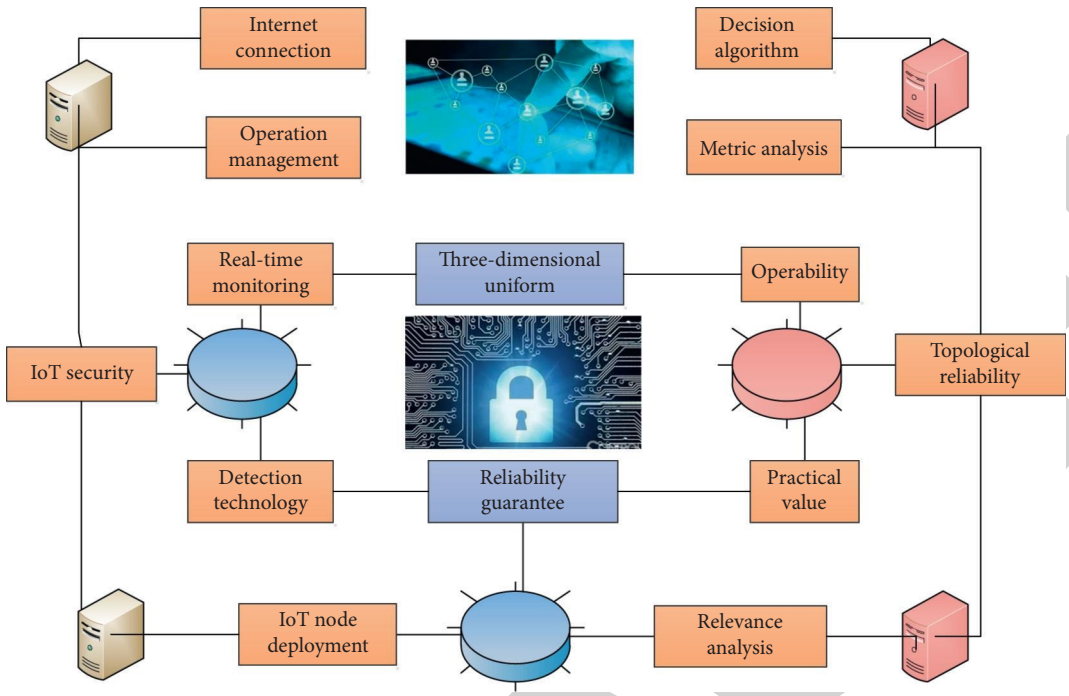

Figure 1: Level display of IoT security detection.

parts: task management platform, mobility management platform, and energy management platform. The distance that can be monitored by the two basic monitoring planes is as follows: when the basic monitoring planes are arranged in sequence, there are IoT security sensor nodes in each horizontal row, the entire distance is divided into n uniform parts, and the length of each part is the sensing radius of the security sensor of the Internet of Things, so the distance that can be monitored by deploying the basic monitoring surface is

$$x(n) = \{x_i\}, \quad i = 1, 2, \ldots, n. \tag{1}$$

When some security sensor nodes of the Internet of Things fail, there may be a blind spot in the original full coverage area. In order to quantify the size of the blind spot caused by node failure, it is first necessary to calculate the area that can be monitored by each basic monitoring surface. $x(n)$ is the given training data set. The node in a basic monitoring surface is a cluster structure, draws a square outside the cluster that is tangent to the sensing area of all nodes in the cluster, and subtracts a number of f areas from the area of the entire square.

$$d(k) = \{d_i(k)\}, \quad i = 1, 2, \ldots, n. \tag{2}$$

Because there will be a g area between every two intersecting circles and the outer tangent line, the circle and the outer tangent line at each corner will form an f area. $d(k)$ is the interval of correct classification according to the classification surface. When the monitoring area is composed of clusters, there are still 4 corners, so there are always 4 areas f, and there are a total of IoT security sensor nodes in each horizontal row, so there are a total of g areas in the entire monitoring area.

$$e = \frac{1}{\lim_{n\longrightarrow\infty} \sum_{i=1}^{n} (d(k) - x(i))}. \tag{3}$$

In the middle row, any common node between the two cluster head nodes is a free node, because removing any of them will have no effect on the coverage of the entire monitoring network. However, if all the two common nodes are removed, a small coverage blind area will appear. Therefore, it can be seen that there is a common node between every two cluster head nodes that is a free node. Therefore, there is the following relationship between the number of free nodes and the number of clusters:

$$h(i) = \frac{\lim_{n\longrightarrow\infty} \sum_{i=1}^{n} w(i)x(i) - b}{\lim_{n\longrightarrow\infty} \sum_{i=1}^{n} w(i)x(i) + b}, \quad h = 1, 2, \ldots, n. \tag{4}$$

The basic principle of the fusion of multiple IoT security sensor information is to make full use of multiple IoT security sensor resources, and through the reasonable control and use of various observational information, the complementary and redundant information can be based on a certain amount of time and space. The combination of these optimization criteria produces a consistent interpretation or description of the observation environment and at the same time produces new fusion results.

$$y(x) = \frac{\lim_{n\longrightarrow\infty} \sum_{i=1}^{n} (w(x) \cdot h(x,k) - b(i))}{\lim_{n\longrightarrow\infty} \sum_{i=1}^{n} (w(x) \cdot h(x,k) + b(i))}, \quad k = 1, 2, \ldots, i. \tag{5}$$

Its goal is to separate observation information based on various IoT security sensors and to derive more effective information by optimizing the combination of information. The ultimate goal is to use the advantages of multiple IoT

security sensors to operate jointly or jointly to improve the entire system. $y(x)$ is the optimal classification surface constructed in the high-dimensional feature vector space. According to the level of data abstraction and target recognition, information fusion is divided into three levels: data level, feature level, and decision level.

$$u = \frac{1}{2m\left(y(x)\cdot x + h(k)\right)^2}. \tag{6}$$

The bottom layer is the terminal grey-associated sensor node deployed in the monitoring area, which is deployed using a star network topology to monitor environmental parameters in real time and form a self-organizing network through communication between nodes. The gateway node is used to control the terminal node, and its role is to realize functions such as network startup and sampling period repair.

2.2. Grey Relational Decision Algorithm. Areas covered by less than 2 in the area they perceive will become blind spots. When a neighboring node fails, the coverage and the area below the area perceived by this node will all become blind areas. Now quantitatively analyze the size of the coverage blind area caused by the failure of different types of nodes. In the large-scale network environment of the Internet of Things, extracting, analyzing, and displaying the security factors that cause changes in the network security status, so as to achieve the purpose of predicting the future development trend, is one of the keys to the evaluation of the security status of the Internet of Things. The coverage of each part of the two basic monitoring surfaces is shown in Figure 2. In the figure, the coverage in the sensing area of the cluster head node is not considered, because once the cluster head node fails, the data of the entire monitoring surface cannot be delivered. Therefore, the cluster head node needs to take more effective measures to ensure its reliable operation. The area covered by the two nodes that compose the constraint node pair is considered to be 1 coverage. By restricting the addition and subtraction of the three basic node failure areas of node pairs, edge nodes, and corner nodes, the smaller 2-cover or 3-cover irregular graph area can be obtained.

In order to solve the problem of SVM parameter selection, this paper uses a PSO-based parameter optimization method. Using this algorithm can achieve a better balance between time-consuming and improved accuracy. On the basis of the network security situation assessment index system constructed in the previous chapter, the index weights are determined according to the grey correlation analysis, the training samples are input to the support vector machine for training, and the improved particle swarm algorithm is used to optimize the parameters of the support vector machine to establish the network. The VC dimension is the core of statistical learning theory. Its definition refers to for an indicator function set, if there are h samples that can be separated by the functions in the function set in all possible 2 h forms, then the function set can be called h when the samples are broken up, and the VC dimension of the function set is the maximum number of samples h that it can break up.

$$w(i,j) = \begin{cases} (w(i) + \min)\cdot f(t), \\ (\max - w(i))\cdot f(t). \end{cases} \tag{7}$$

The size of the VC dimension indicates the strength of the learning ability of the method, and the larger the dimension is, the stronger the learning ability is. Statistical learning theory is a method to study the correlation between actual risk (i.e., expected risk) and empirical risk (i.e., training error) in function concentration, and it is also called the generalized boundary. For the research on this issue, it is now generally agreed that, for all functions in the indicator function set, the empirical risk and the actual risk satisfy the following relationship at least with a probability of $1-\eta$.

$$z(i) = \overline{y}(i) - y(i) = \lim_{n\longrightarrow\infty}\sum_{i=1}^{n} w(i)\cdot y(i). \tag{8}$$

Under the condition of limited training samples, the confidence range has a positive correlation with the VC dimension of the learning machine. The VC dimension increases with the increase of the confidence range, which will also cause the difference between the empirical risk and the real risk to become larger. At the same time, this is also the reason for the phenomenon of overlearning in learning machines. In the process of machine learning, it is necessary to have a good generalization of future samples and to make the empirical risk and actual risk small; it is necessary to control the VC dimension as much as possible to narrow the confidence range.

$$\begin{aligned} \min Y &= \frac{\lim_{n\longrightarrow\infty}\sum_{i=1}^{n} w(i)\cdot\left(y(i,t) - y(t)\right)}{2}, \\ R &= \sqrt{\frac{\lim_{n\longrightarrow\infty}\sum_{i=1}^{n}\left(x(i)-x\right)^2}{y(x)-x}}. \end{aligned} \tag{9}$$

In order to solve this problem, the statistical learning theory proposes a new solution strategy, which is to replace the function set with the decomposed function subsequence set.

2.3. Optimization of Safety Detection Model Parameters. The main components of the monitoring system are as follows. (1) Key nodes (cluster head nodes and gateway nodes): when the two kinds of nodes are used, the cluster head nodes are distributed in the roadway, and only the grey correlation communication function is enabled, while the gateway nodes are distributed in the roadway entrance and the main roadway, and the two communication methods of wired and grey correlation are enabled to realize the grey correlation of the Internet of Things. Therefore, when analyzing and researching grey systems, the key to solving such problems is how to find correlation and correlation metrics from random time series so as to perform factor analysis and provide a basis for decision-making. The data gathered by the security sensor node are exchanged with the base station

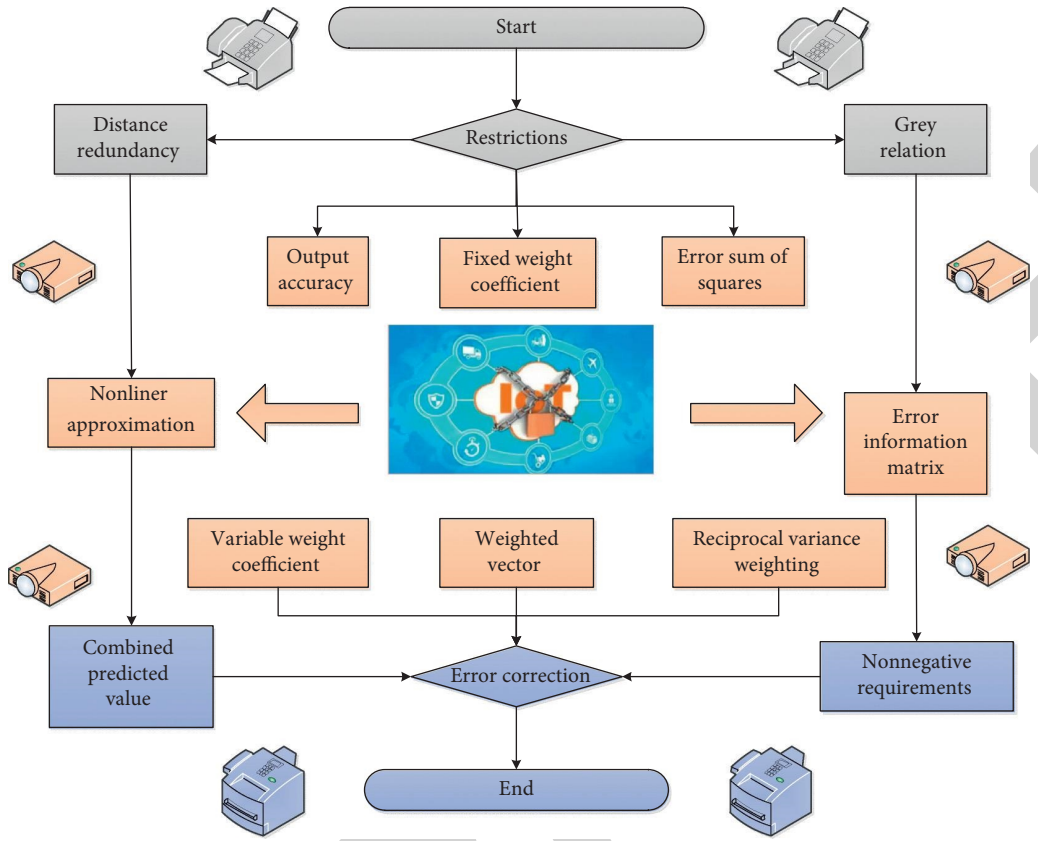

Figure 2: Grey relational decision algorithm flow.

data. (2) IoT security sensor node: it is responsible for collecting environmental data in the monitoring area, sending the data to neighboring nodes through grey correlation communication, and finally converging to key nodes.

There are eight common nodes around the cluster head node. The height of each row of nodes on the wall increases by 1/4 of the wall height. Placing the cluster head node in the center has two advantages: (1) making the distance between the common nodes in the cluster and the cluster head node as equal as possible to achieve a relatively balanced energy consumption of each node; (2) placing the cluster head node of the center which is beneficial to protect the cluster head nodes. In the IoT monitoring scenario, if there is gravel on the top plate, it is likely to damage the IoT security sensor nodes, and the IoT security sensors in the top row can affect the cluster head nodes. To be a certain degree of protection, an IoT security sensor on the top board does not belong to any basic monitoring surface. It has both monitoring and routing functions. In IoT mines, the roof of the roadway is generally curved, and monitoring the pressure of the roof is of great significance for preventing roof fall accidents.

At the same time, after the IoT security sensors at the top board communicate with each other, a path to the sink node is formed, which is beneficial to improve the forwarding speed of data packets. After connecting multiple basic monitoring bodies, the monitoring network of the entire roadway is obtained. It shows the connection of four basic monitoring bodies. When using the Internet of Things to monitor major hazards of the Internet of Things, the accuracy of the monitoring data determines the practicability of the monitoring system. The accuracy of monitoring data is related to the deployment method and density of IoT security sensor nodes. In the 1-coverage problem, the hexagonal deployment strategy is an optimal deployment strategy, because the hexagonal deployment uses the least number of nodes for each monitoring area coverage, as shown in Figure 3. However, in the monitoring of major hazards in the Internet of Things, due to the limited height of the roadway, it is impossible to make any six nodes into a hexagon, but they can only be deployed along the roadway.

On the basis of research on situational awareness and risk assessment, in accordance with relevant national standards and regulations, the security situational awareness process is the main line, with emphasis on the three key links of situation understanding, situation assessment and situation prediction, and the network security situation based on PSO and SVM. Based on the evaluation technology and the situation prediction technology of the improved Elman grey relational decision model, a hierarchical network security situation awareness model framework is established, as shown in Figure 4. Situation understanding is the basis of situation awareness.

Situation understanding is mainly to complete the preprocessing of raw data and prepare for the next stage of situation assessment, which mainly includes asset

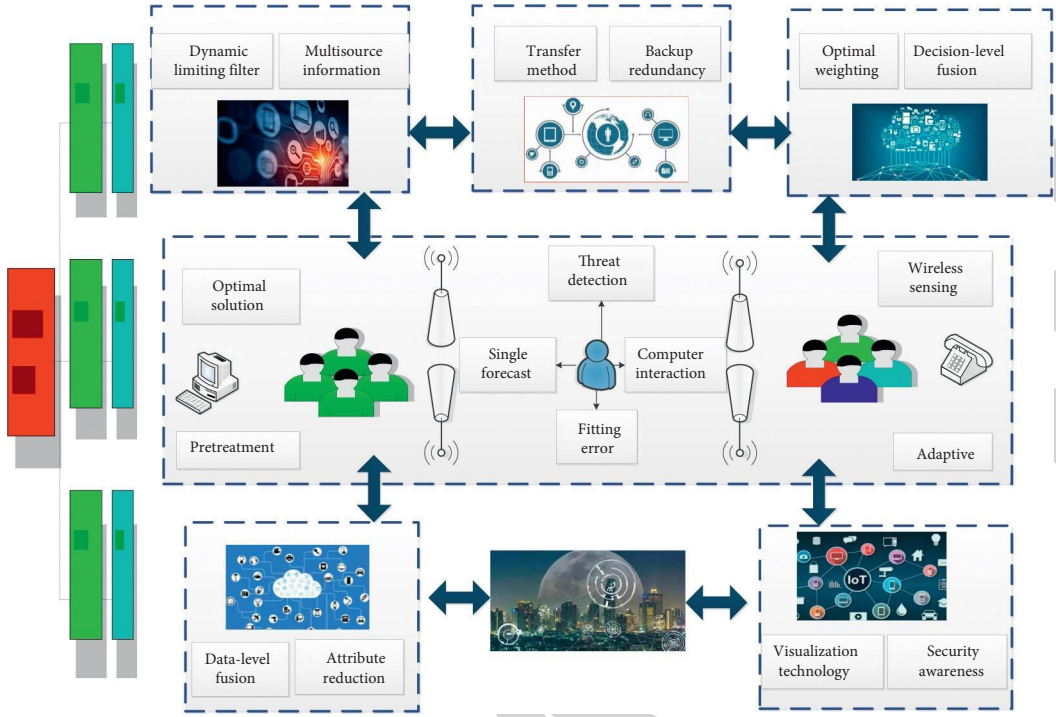

Figure 3: The framework of IoT security detection model.

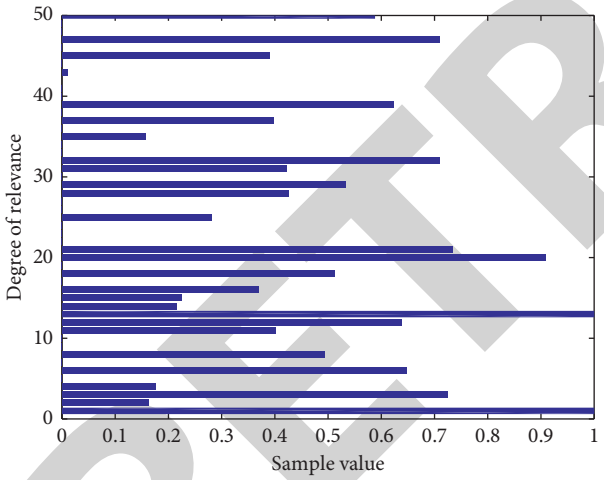

Figure 4: Sample correlation distribution of grey correlation algorithm.

identification, vulnerability identification, and threat detection. Situation assessment is the core of situation awareness. In this paper, a situation assessment method based on SVM and PSO is used to improve the particle swarm algorithm to optimize the support vector machine parameters. Using this algorithm can achieve a better balance between time-consuming and improved accuracy and improve the effect of situation assessment. Situation prediction is the essential requirement of situation awareness. As a real-time dynamic system of the Internet of Things, the use of grey correlation method to analyze its network security status has good operability and practical value. This paper constructs a network security situation prediction model based on the relevant theories of the grey relational decision-making model, referring to the double-feedback Elman grey relational decision-making model, optimizes the parameters through adjustment factors, and constructs a double-feedback Elman grey relational decision-making model based on the adjustment factors. The network security situation prediction model improves the effect of situation prediction.

3. Application and Analysis of IoT Security Detection Model Based on Grey Relational Decision Algorithm

3.1. Quantification of IoT Security Assessment Indicators. Two models are used to predict the situation value separately. Every 6 data are a group, the first 5 data are used as the prediction input, and the sixth data is the prediction output, starting from the 96th day, that is, from the 96th to the 100th situation value on the 101st day and so on. The prediction result is shown in Figure 5. The disadvantage of this method is that when the number of subsets is too large, the time overhead of the algorithm is too large; the second is to design a certain structure of the function set so that each subset can obtain the smallest experience risk (such as making the training error 0). It takes 6 iterations of calculation to reach the expected minimum error; the error of the GA-BP algorithm for training the grey relational decision-making model continues to decrease over time, and the test error curve and the verification error curve maintain a roughly similar trend. When it is trained to the circle in the figure, the generalization error of the network is minimized, which is the optimal weight threshold of the grey relational decision-

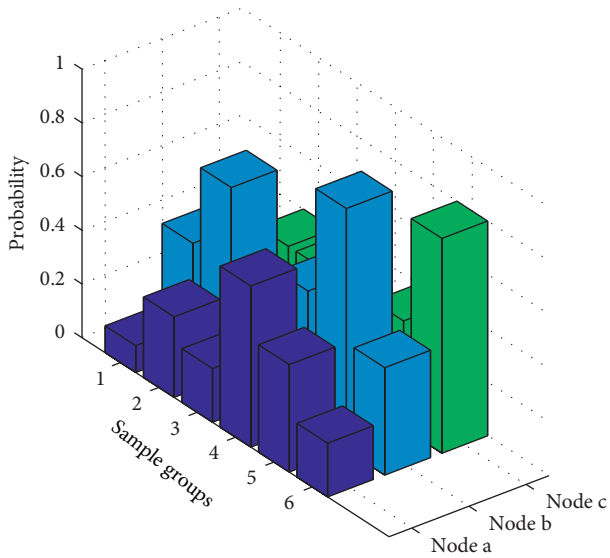

Figure 5: Histogram of probability distribution of IoT nodes.

making model. The GA-BP algorithm has a fast convergence speed, because the population evolution requires sufficient time, and the population size, number of iterations, and the initial range of the weight threshold also have a greater impact on the convergence time of network training.

Based on the BP grey relational decision-making model group and the BP grey relational decision-making model combinator, the dual BP grey relational decision-making model-intelligent neural network classifies the combined model and uses the hybrid method to combine the output results of the three optimized BP grey relational decision-making models. The rate of evolution is slow. Collect and statistically detect the attack data on the network within the time period T. According to the performance of the entire system and the actual situation, the size of the time period T can be adjusted accordingly. Generally, the crossover probability is set to a larger value in the range of [0.4, 1], which can not only expand the optimization space but also improve the efficiency of the algorithm, so as to realize the ability of the genetic algorithm to search for the optimal solution globally. If the error is greater than the expected error value, the two processes need to be repeated to achieve the target accuracy. The disease output vector of the decision model is fitted and trained until the prediction accuracy requirements are met, so as to achieve the purpose of predicting the disease of the grey relational decision model. In the following, the grey relational decision-making model displacement and the grey relational decision factor are, respectively, used to predict the two diseases using the grey neural network prediction model based on wavelet correlation. Through the comparison and analysis of deformation monitoring data prediction, it can be seen that the fitting accuracy of the intelligent grey relational decision-making model is significantly better than that of other single models, and the fitting accuracy can be improved by more than 40%.

The experiment is to obtain 20 sets of measured data of IoT security sensing under 5 types from the associated decision database of an Internet of Things and extract the corresponding feature vector samples after wavelet packet decomposition processing, which is used to compare the trained neural network. It can be seen from Figure 6 that using the design method of this paper to detect the security sensor nodes of the Internet of Things can effectively reduce the false alarm rate and the false alarm rate of the diagnostic system and significantly improve the robustness of the diagnostic system.

3.2. Matrix Simulation of Safety Detection Model. Under the same learning sample and initialization parameters, the effect of the optimization algorithm is analyzed from the number of iterations and whether it falls into a local minimum. Set the maximum step size of BP grey relational decision model training to 10000, and the expected minimum error is 101. It is feasible and effective to use the combined model to predict the displacement. It also proves the hysteresis characteristics of the data based on displacement and environmental factors. Perform dimensionless processing on the above-stated data table, and obtain its grey incidence matrix according to the relevant formula (the formula is omitted here due to space limitation), and the relevant grey correlation coefficient value is obtained. After the wavelet time-lag correlation is used to analyze the time lag of the data, the WGRFM model is used to predict the displacement of the stone grey relational decision model. It is more effective and accurate. The accuracy line graph of grey correlation attributes is as shown in Figure 7.

First, the disease time series and the environmental factor time series are preprocessed, and on the basis of correlation analysis, n key environmental dependent variables are analyzed; the wavelet correlation theory is used to construct the wavelet time-lag correlation function, the disease, and the key environment. It can be seen that the prediction accuracy of the optimized model of the optimized Elman grey relational decision model is higher than that of the original Elman grey relational decision model, and the running time of the prediction algorithm is less than that of the original Elman grey relational decision model. It is higher than other time periods, and it should arouse the attention of network managers and take necessary preventive measures.

According to the conclusion of the analysis, the grey correlation decision factor has the greatest correlation with the safety false alarm data. Therefore, the lagging cross-correlation analysis is carried out on this key influencing factor and the grey correlation decision factor disease, and the value range of the lag factor k is selected from 0 to 20. The result is shown in Figure 8. The safety false alarm data affect the displacement when $k = 15$. According to the abovementioned various attack hazards, combined with the weights given by the expert system, the network security status index value is calculated. The maximum of the grey correlation decision factor has the greatest impact on the displacement when $k = 17$.

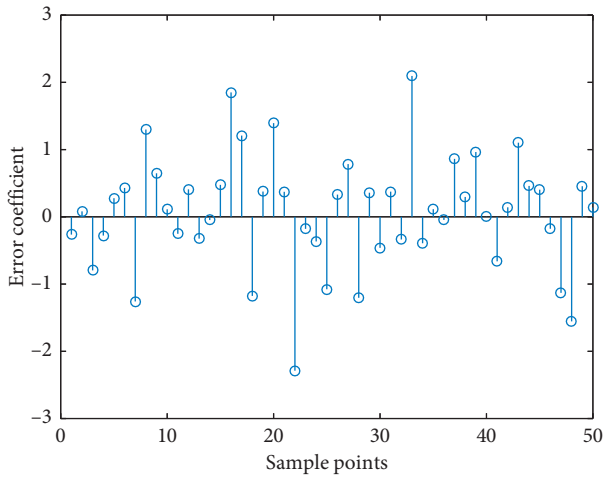

Figure 6: Error factor matchstick diagram of different sample points of the model.

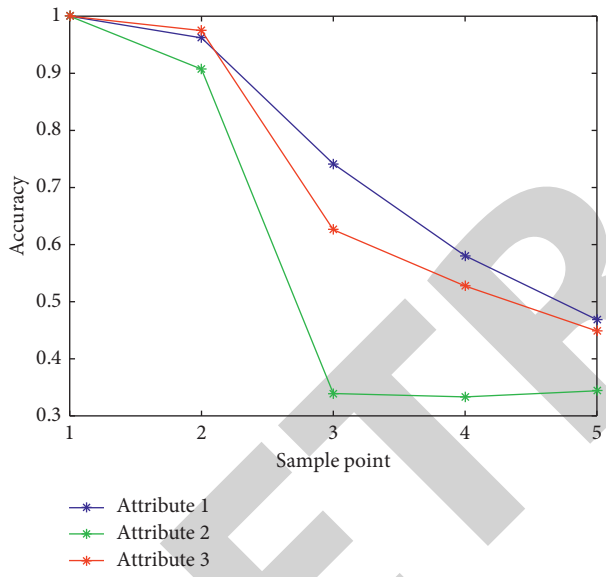

Figure 7: Accuracy line graph of grey correlation attributes.

WGRFM forecasting models can be trained to fit the details of the changes in the time series of grey correlation decision factors.

The network security risk index value is calculated according to the weight of the above-mentioned various attacks. It can be seen in Figure 9 that the WGRFM training error is the smallest. The Shannondwave of the force Hamming window is used as the mother wavelet to perform wavelet packet decomposition on the output signal of the Internet of Things security sensor. Because the time-domain waveform tends to 0 faster than the Shannond wave, the waveform attenuates rapidly, and the support is small. Effectively, it improves the accuracy of numerical calculations, the time-domain truncation after the Hamming window has little effect on the frequency domain, and the Gibbs phenomenon will not occur in the frequency domain.

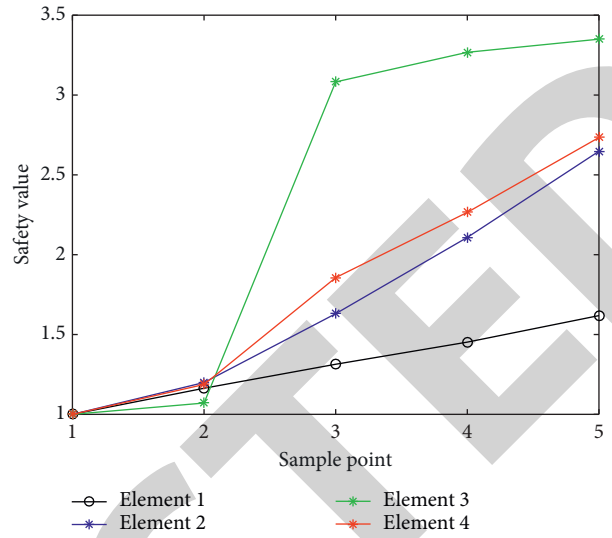

Figure 8: The distribution of safety detection values of different sample elements.

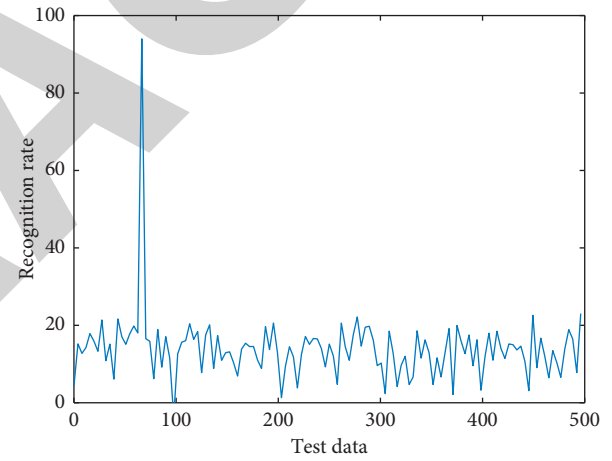

Figure 9: The distribution of the recognition rate of test samples.

3.3. Example Results and Analysis. The development environment includes a computer with a CPU speed of 2.0 GHz and above, memory not less than 2G, and hard disk space not less than 50G; system development tool including Eclipse platform and jdk1.7.0_25 development kit; web server using Tomcat6.0; database using SQL Server 2008; web browser adopting IE6.0 and above; website development languages and tools including web design tools, system architecture tools, programming languages, and database languages.

Among them, the page design is HTML language, JSP technology, JavaScript technology, CSS language, and Highcharts plug-in; the back-end architecture adopts framework construction environment; dynamic implementation languages include Java language, JavaEE platform, Jquery, and Ajax; database query language; SQL language. According to the above-obtained network security index value analysis, the security status of the network can be obtained. It can be seen from the lag correlation number in

Figure 10 that the correlation between the time series of key meteorological elements and the displacement is constantly changing with the change of the lag factor. Among them, the influence of the surface temperature on the displacement is at the lag factor k, the safety false alarm data have the greatest impact on the displacement when $k = 19$, and the grey correlation decision factor has the greatest impact on the displacement when $k = 17$. Smoothing filtering preprocessing of the collected data is often superimposed with noise due to various reasons so that the characteristic information of the time series is often submerged in the noise. In order to be able to restore the real signal, it is necessary to perform signal preprocessing such as filtering.

In RBF training and prediction, select the first row to the 30th row as the training samples and start the prediction from the 4th and the 31–35 behavior prediction test samples. In order to enhance the accuracy of the prediction, before the RBF training, all the data were normalized, and the results of three sequences were obtained. Input to the RBF grey relational decision-making model for learning and training, and the displacement fitting sequence obtained is shown in Figure 11. According to the impact of various attacks on the security of the network system, the weight can be selected in combination with the expert system. There are 5 evaluation levels, so the dimension of the input layer is 20, the output layer is a single factor, and the output dimension is 5. If the input is all normal, that is, the input vector is (1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, l, 0, 0, 0, 0), the output must also be normal, that is, the output vector is (1, 0, 0, 0, 0); if all the inputs are basically normal, that is, the input vector is (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, l, 0, 0, 0), it can be inferred that its output must be basically normal, that is, the output vector is (0, l, 0, 0, 0).

For performance comparison, a single-factor RBF grey relational decision model, Verhulst-RBF combined forecasting model, and GM-grey relational decision model combined model were established to fit and predict the displacement. This is consistent with the changing trend of actual engineering and basically consistent with the empirical judgment of experts, indicating that it is reasonable to apply the grey relational decision model to the deformation safety evaluation of the Internet of Things.

It can be seen that the prediction results obtained by the GM-RBF grey correlation decision model prediction algorithm based on wavelet correlation are the closest to the true value, followed by the GM-RBF grey correlation decision model algorithm based on wavelet correlation. In the fitting process, it can fit the details of the curve well. The training effect of the design model and other models is shown in Figure 12. The solutions of the two sequential differential equations correspond one-to-one, respectively. The output data of the GM (1, 1) model are normalized, and the data of the previous 27 days are used as training data. The GM (1, 1) model can basically show the trend of grey relational decision-making factors, but the error is very obvious; the GM-grey relational decision model and the grey-grey relational decision-making model can basically fit the grey relational decision-making well. Among them, in the GM-grey relational decision model, the grey relational decision model

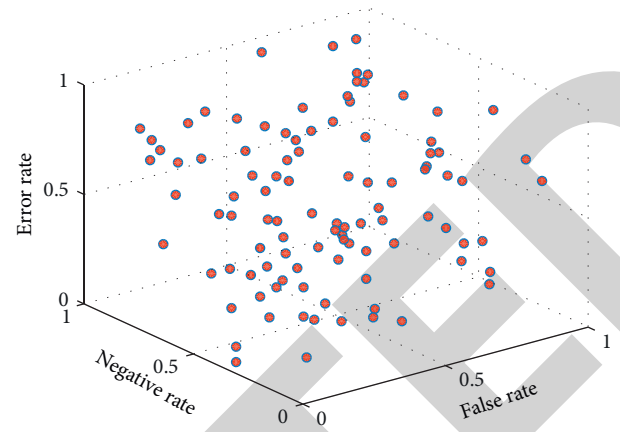

Figure 10: Three-dimensional scatter point distribution of sample tolerance rate.

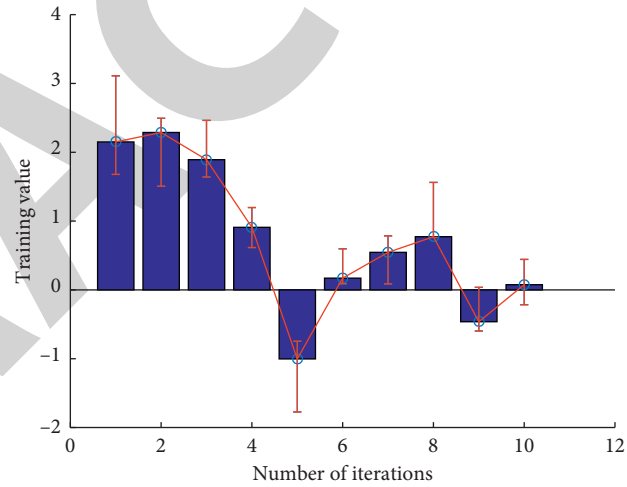

Figure 11: The sample training value depends on the number of iterations.

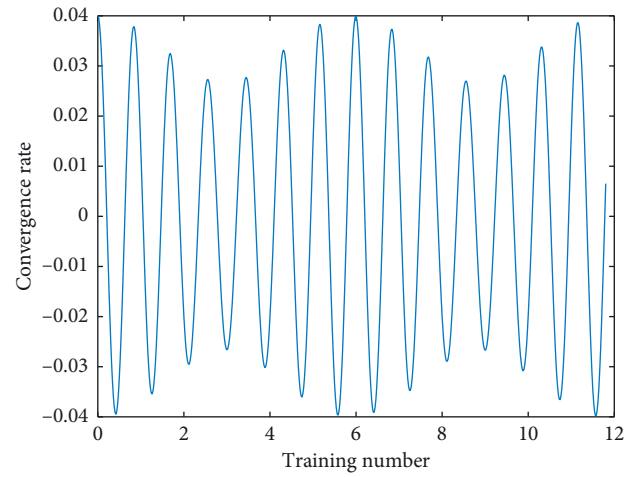

Figure 12: The relationship between sample security detection conversion rate and training times.

network adopts a 6-6-1 three-tier structure. The transfer function of the grey relational decision model is Sigmoid, the learning rate is 0.02, and the maximum number of iterations is 100. According to the grey relational decision-making model trained by the standard BP algorithm, DZ-BP algorithm, LM-BP algorithm, and GA-BP algorithm under the same sample data, the four-phase data are selected as the predictive output of the model, and the data of the four-phase grey relational decision-making model are compared effect. LM-BP is one of the standard numerical optimization methods to accelerate the convergence of the BP algorithm. The Jacobian matrix (easy to calculate) is used to replace the calculation of the Hessian matrix, which improves the optimization efficiency. Genetic algorithm is abstracted from Darwin's theory of evolution. Although we would doubt the truthfulness of Darwin's theory of evolution, the genetic algorithm can indeed be said to be a very good global optimization algorithm. As shown in it, the original curve of the standard BP grey relational decision model (upper left) is quite different from the model prediction curve. The maximum error value reaches 0.1226, and the sum of squared errors is 0.0247. Its maximum error value is 0.6488, and the sum of squares of errors is 0.0115, which can improve the standard BP grey to a certain extent. The relatively small value of the network security index indicates that the threat to the network during this time period is higher than that of other time periods, and the network administrators should pay great attention to it and take necessary preventive measures. The fitting accuracy of the associated decision-making model is good. The maximum error value of the GA-BP grey associated decision-making model is 0.1221, and the sum of squared errors is 0.0227. The optimization effect of its fitting accuracy is not better than that of DZ-BP and LM-BP.

It can be seen from Figure 13 that the two combined models of Verhulst-RBF and grey relational decision-making model can better fit the development and changes of the displacement series and have a better fitting effect. It can be seen that the average error of grey relational decision-making factor prediction is 0.69, and the relative error is 6.9%. It can be seen from the above chart that the fitting effect of the standard grey relational decision-making model is relatively poor, and the optimized grey relational decision-making model can be greatly improved in accuracy. Through the above examples, it can be seen that the evaluation results obtained by the grey theory-based IoT security status evaluation method given in this paper are still relatively in line with the actual situation. From the data, the error indicators of the respective models can be obtained. The root mean square error of the grey relational decision-making model is large. The average root mean square error of the optimized grey relational decision-making model is smaller than that of the grey relational decision-making model neural network, while the mean square of the combined model is better than the dual grey relational decision-making model. The learning sample is obtained by permutation and combination of each evaluation factor. The sample dimension is the product of the number of evaluation indexes and the number of evaluation grades, and the number of samples is the power of the number of evaluation indexes of

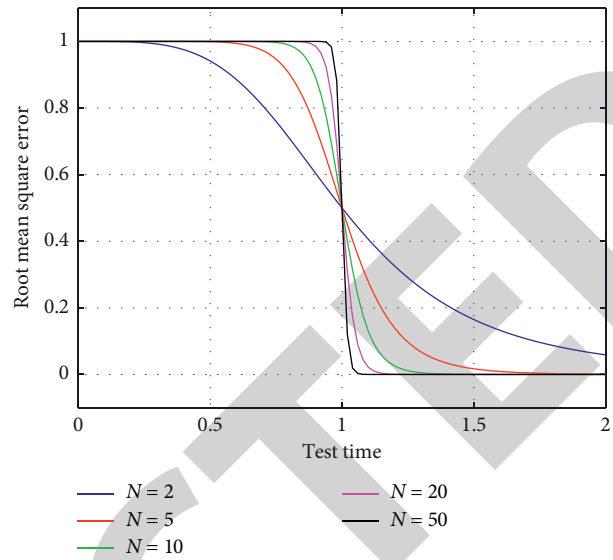

Figure 13: The root mean square error of the sample output value varies with the number of tests.

the evaluation grades. The dual grey relational decision-making model of the combined model is more significant in improving the accuracy of the single model and can improve the fitting accuracy by more than 45%.

4. Conclusion

This paper analyzes the four failure modes of IoT security sensors in the monitoring and control system and establishes a fault diagnosis strategy for IoT security sensors on this basis. Aiming at the four types of invisible soft faults that are common in IoT security sensors, namely, constant, drift, offset, and periodic, which are based on wavelet analysis and FRBF grey relational decision-making model, the feature energy spectrum extracted by wavelet packet decomposition is proposed. An IoT security sensor node fault diagnosis method for pattern classification and identification with the grey correlation decision model is optimized with the extended Kalman filtering algorithm (EKF). The output signal of the security sensor of the Internet of Things is decomposed by wavelet packet, and the local discriminant basis (LDB) algorithm based on the cost function is used for cropping to obtain the optimal feature energy spectrum, which is processed as a feature vector to train the EKF-FIF grey correlation. The decision model adopts parameter augmentation and statistical dynamics methods and uses EKF parameter estimation with tuning factors to identify the fault type of the IoT security sensor node. Experiments show that the identification accuracy of this method is more than 95%, the false alarm rate and true alarm rate are significantly better than other algorithms, and it can be effectively used for the online fault diagnosis of IoT security sensor nodes in the IoT system. The fault recognition accuracy rate is more than 95%. The training root mean square error and the test root mean square error show better robustness and stronger classification ability, which can significantly improve the effectiveness and accuracy of fault diagnosis. Applying the

diagnostic algorithm to the online fault detection of IoT security sensor nodes in the Internet of Things network, it can quickly identify 4 types of hidden soft and soft faults, has good generalization ability, and can be effectively used in the Internet of Things security in the Internet of Things system. The online fault diagnosis of sensor nodes can greatly improve the working reliability and anti-interference ability of the Internet of Things monitoring system.

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 conflicts of Interest.

References

[1] K. Zhao and L. Ge, "A survey on the internet of things security," *Computational Intelligence and Security*, vol. 20, no. 13, pp. 663–667, 2020.

[2] Y. Chahid, M. Benabdellah, and A. Azizi, ""Internet of things security," wireless technologies," *Embedded and Intelligent Systems*, vol. 6, no. 21, pp. 1–6, 2018.

[3] M. Banerjee, J. Lee, and K. Choo, "A blockchain future for internet of things security: a position paper," *Digital Communications and Networks*, vol. 4, no. 13, pp. 149–160, 2018.

[4] N. Nesa, T. Ghosh, and I. Banerjee, "iGRM," *ACM Transactions on Knowledge Discovery from Data*, vol. 12, no. 4, pp. 1–23, 2018.

[5] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The future of healthcare internet of things: a survey of emerging technologies," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1121–1167, 2020.

[6] S. Goudarzi, M. H. Anisi, A. H. Abdullah, J. Lloret, S. A. Soleymani, and W. H. Hassan, "A hybrid intelligent model for network selection in the industrial Internet of Things," *Applied Soft Computing*, vol. 74, no. 4, pp. 529–546, 2019.

[7] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in internet of things: challenges, solutions and future directions," *Electronics*, vol. 9, no. 7, p. 1177, 2020.

[8] M. Habib, I. Aljarah, and H. Faris, "A modified multi-objective particle swarm optimizer-based Lévy Flight: an approach toward intrusion detection in internet of things," *Arabian Journal for Science and Engineering*, vol. 45, no. 8, pp. 6081–6108, 2020.

[9] F. Castaño, S. Strzelczak, and A. Villalonga, "Sensor reliability in cyber-physical systems using internet-of-things data: a review and case study," *Remote Sensing*, vol. 11, no. 19, pp. 22–25, 2019.

[10] H. Han, J. Li, and X. Chen, "The individual identification method of wireless device based on a robust dimensionality reduction model of hybrid feature information," *Mobile Networks and Applications*, vol. 23, no. 4, pp. 709–716, 2018.

[11] A. Mellit and S. Kalogirou, "Artificial intelligence and internet of things to improve efficacy of diagnosis and remote sensing of solar photovoltaic systems: challenges, recommendations and future directions," *Renewable and Sustainable Energy Reviews*, vol. 4, no. 43, pp. 11–19, 2021.

[12] A. Aziz, W. Osamy, and M. Khedr, "Grey Wolf based compressive sensing scheme for data gathering in IoT based heterogeneous WSNs," *Wireless Networks*, vol. 2, no. 20, pp. 1–24, 2018.

[13] E. Kougianos, S. Mohanty, and G. Coelho, "Design of a high-performance system for secure image communication in the internet of things," *IEEE Access*, vol. 6, no. 4, pp. 1222–1242, 2019.

[14] M. Sattarian, J. Rezazadeh, R. Farahbakhsh, and A. Bagheri, "Indoor navigation systems based on data mining techniques in internet of things: a survey," *Wireless Networks*, vol. 25, no. 3, pp. 1385–1402, 2019.

[15] S. Alharbi, P. Rodriguez, and R. Maharaja, "FOCUS: a fog computing-based security system for the Internet of Things," *IEEE Annual Consumer Communications*, vol. 3, no. 4, pp. 1–5, 2019.

[16] K. Deng, L. Xing, and M. Zhang, "A multiuser identification algorithm based on Internet of Things," *Wireless Communications and Mobile Computing*, vol. 2, no. 9, pp. 32–49, 2019.

[17] M. Swan, "Sensor the internet of things, wearable computing, objective metrics, and the quantified self 2.0," *Journal of Sensor and Actuator Networks*, vol. 2, no. 12, pp. 217–253, 2019.

[18] M. Javaid and I. Khan, "Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic," *Journal of Oral Biology and Craniofacial Research*, vol. 5, no. 5, pp. 209–214, 2021.

[19] B. L. Risteska Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: challenges and solutions," *Journal of Cleaner Production*, vol. 140, no. 14, pp. 1454–1464, 2017.

[20] W. Li, W. Meng, and M. H. Au, "Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments," *Journal of Network and Computer Applications*, vol. 161, no. 16, Article ID 102631, 2020.

[21] N. Nesa, T. Ghosh, and I. Banerjee, "Non-parametric sequence-based learning approach for outlier detection in IoT," *Future Generation Computer Systems*, vol. 82, no. 82, pp. 412–421, 2018.

[22] S. Balamurugan, A. Ayyasamy, and K. Joseph, "Enhanced petri nets for traceability of food management using internet of things," *Peer-to-Peer Networking and Applications*, vol. 2, no. 14, pp. 30–41, 2021.

[23] Z. Zhang, Y. Li, and C. Wang, "An ensemble learning method for wireless multimedia device identification," *Security and Communication Networks*, vol. 20, no. 8, pp. 14–22, 2018.

[24] M. Safaei Pour, A. Mangino, K. Friday et al., "On data-driven curation, learning, and analysis for inferring evolving internet-of-Things (IoT) botnets in the wild," *Computers & Security*, vol. 91, no. 91, Article ID 101707, 2020.

[25] X. Lin, P. Lin, and E. Yeh, "Anomaly detection/prediction for internet of things: state-of-the-art and the future," *IEEE Network*, vol. 4, no. 1, pp. 23–37, 2020.

[26] H. Ma and X. Pang, "Research and analysis of sport medical data processing algorithms based on deep learning and Internet of Things," *IEEE Access*, vol. 7, no. 7, pp. 118839–118849, 2019.

[27] B. Li, R. Liang, W. Zhou, H. Yin, H. Gao, and K. Cai, "LBS meets blockchain:an efficient method with security preserving trust in SAGIN," *IEEE Internet of Things Journal*, p. 1, 2021.

[28] J. Zhang and G. Qu, "Physical unclonable function-based key sharing via machine learning for IoT security," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 8, pp. 7025–7033, 2019.

[29] W. Wang, N. Kumar, J. Chen et al., "Realizing the potential of the internet of things for smart tourism with 5G and AI," *IEEE Network*, vol. 34, no. 6, pp. 295–301, 2020.

[30] 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, Article ID 107275, 2020.

[31] J. Yang, J. Zhang, and H. Wang, "Urban traffic control in software defined internet of things via a multi-agent deep reinforcement learning approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3742–3754, 2021.

[32] S. Yang, T. Gao, J. Wang et al., "Efficient spike-driven learning with dendritic event-based processing," *Frontiers in Neuroscience*, vol. 15, p. 97, 2021.

[33] M. Chen, S. Lu, and Q. Liu, "Uniqueness of weak solutions to a Keller-Segel-Navier-Stokes model with a logistic source," *Applications of Mathematics*, pp. 1–9, 2021.

[34] F. Lu and J. Q. Huang, "Feature extraction algorithm of clustering based on grey relational theory," *Systems Engineering-Theory & Practice*, vol. 32, no. 4, pp. 872–876, 2012.

[35] M. Golfarelli and S. Rizzi, "A model-driven approach to automate data visualization in big data analytics," *Information Visualization*, vol. 19, no. 1, pp. 24–47, 2020.