Hindawi
Journal of Sensors
Volume 2022, Article ID 5013905, 10 pages
https://doi.org/10.1155/2022/5013905

Research Article

A Data-Driven WSN Security Threat Analysis Model Based on Cognitive Computing

Xinyan Huang

School of Computer Science and Technology, Shandong University of Finance and Economics, Shandong Jinan 250014, China

Correspondence should be addressed to Xinyan Huang; 20063462@sdufe.edu.cn

Received 24 November 2021; Revised 21 December 2021; Accepted 22 December 2021; Published 27 January 2022

Academic Editor: Gengxin Sun

In this paper, we use cognitive computing to build a WSN security threat analysis model using a data-driven approach and conduct an in-depth and systematic study. In this paper, we develop a simulation platform (OMNeT++-based WSN Security Protocol Simulation Platform (WSPSim)) based on OMNeT++ to make up for the shortcomings of current WSN simulation platforms, improve the simulation capability of WSN security protocols, and provide a new technical means for designing and verifying security protocols. The WSPSim simulation platform is used to simulate and analyze typical WSN protocols and verify the effectiveness of the platform. In this paper, we mainly analyze the node malicious behavior by listening and judging the communication behavior of the nodes, and the current trust assessment is given by the security management nodes. When the security management node is rotated, its stored trust value is used as historical trust assessment and current trust assessment together to participate in the integrated trust value calculation, which improves the reliability of node trust assessment; to increase the security and reliability of the management node, a trust value factor and residual energy factor are introduced in the security management node election in the paper. According to the time of management node election, the weights of both are changed to optimize the election. Using the WSPSim simulation platform, a typical WSN protocol is simulated and analyzed to verify the effectiveness of the platform. In this paper, the simulation results of the LEACH protocol with an MD5 hash algorithm and trust evaluation mechanism and typical LEACH protocol as simulation samples are compared; i.e., the correctness of the simulation platform is verified, and it is shown that improving the security of the protocol and enhancing the security and energy efficiency of wireless sensor networks provide an effective solution.

1. Introduction

A wireless sensor network (WSN) is a key technology for IoT and has been widely used in many fields. WSN is characterized by many sensor nodes and a large network size, which is usually deployed in an exposed external environment and therefore vulnerable to various forms of attacks [1]. Authentication is the basis for securing the network, and traditional authentication mostly uses centralized authentication, but such an authentication mechanism has many drawbacks: the security of the network depends entirely on the authentication center, and once the authentication center is maliciously attacked, the whole authentication system will fall into collapse; when the scale of the network is expanded, the performance of the network will be affected due to the limited computing power and storage capacity of the authentication center. With the development of WSN, the topology of the network is ever-changing, and centralized authentication is not flexible enough. Therefore, the security of centralized authentication is not high and scalability is poor. This security problem can be effectively solved by establishing a distributed trust model in WSN [2].

With the rapid development of information technology, the Internet of Things has come into being. IoT is an application expansion based on the Internet, which extends its application end from the object to object, enabling information exchange and communication between people and things. The wireless sensor network is the key technology of IoT, which is oriented to the perception layer in the three-layer structure of IoT [3, 4]. The wireless sensor network is a new multihop self-organizing network composed of numerous sensor nodes with the characteristics of overall sensing, reliable transmission, and intelligent processing. The data acquisition unit is responsible for collecting information in the monitoring area and converting it; the data transmission unit mainly sends and receives that collected data information in the form of wireless communication [5]. To establish a wireless sensor network environment, many sensors, a data transmission center, and a base station are required. Sensors are devices with detection, computing, and communication capabilities. Wireless sensor networks integrate the acquisition, processing, and execution of information with sensing, processing, communication, and storage functions and can measure indicators [6]. Wireless sensor networks have a wide range of applications in many fields such as military battlefield and smart home with their self-organization and fast deployment. Due to the limited computing resources and long-term operation of the IoT sensor device nodes converged and accessed by the edge computing terminal, the traditional "patch" security reinforcement mechanism cannot be applied to the IoT sensor device node and the IoT sensor device in an uncontrolled environment. The risk of malicious use of nodes is extremely high, making edge computing terminals extremely easy to become attack targets or springboards for IoT sensor device nodes.

In the era of big data, improving the cognitive ability of large-scale data is an urgent need for technological development. Cognitive computing is a set of theoretical studies that includes the whole process from the sample input, processing, and output. Cognitive computing is based on mathematical methods, computer technology, and biological neurology, and it can analyze data by simulating the mechanism of the human brain [7]. The application of cognitive computing for data value mining will help people to discover potential laws and improve the way they work. In the era of big data, it is of great practical importance to study the cognitive ability of knowledge acquisition and experiential learning for massive data [8].

2. Related Works

The research on wireless sensor networks first started in the 1970s and 1980s, and with the rapid development of the Internet, wireless sensor networks have also been developed. Centralized authentication is generally used in traditional networks for authentication, thus ensuring network security. The communication parties identify each other with the help of an authoritative authentication center to establish a trust relationship. The structure of centralized authentication is relatively simple, so there are many problems: the security of the entire network depends on this authentication center, and the authentication center is easily identified by malicious nodes and attacked; there is a great security risk; in the case of large network size and limited performance of the authentication center, the network may collapse at any time [9]. There are many sensor nodes in the WSN, the node topology is very variable, and the centralized authentication is not flexible enough to meet this variable topology. WSN has become one of the key technologies for information access in the information age, attracting close attention from academia and industry, and has become a research hotspot in the fields of automation, computing, and communication. WSN is listed as one of the top ten technologies that will change the world in the 21st century and is also listed as one of the four new technologies in the future. At present, with the widespread promotion of the Internet of Things and "Internet Plus," the application research of WSN has entered a new climax [10].

The trust management approach, first proposed in 1996, is based on a simple language that specifies trust operations and trust relationships and solves the problem of trusting one node over another by developing a security policy and delegating it to third-party nodes; it also follows the principles of uniformity, flexibility, locality control, and separation of mechanisms and policies to develop a general framework that can be applied to any service that requires encryption [11]. The approach considers the dynamic variability of nodes in the network and meets the open needs of the network. Based on this, scholars have proposed trust models such as EigenTrust, Peer Trust, and Power Trust, all of which have improved the calculation related to trust values to some extent. Although these trust models are more accurate in the calculation of trust values, the structure of many of them does not apply to wireless sensor networks [12].

With the continuous changes of attack methods, the concealment of malicious attacks has become stronger and stronger. On the one hand, terminal identity execution authentication and identification technology has been easily forged or bypassed; on the other side, legitimate terminals that have passed identity authentication are used as a springboard; it is difficult to detect and identify infiltration attacks. As the network security situation becomes increasingly complex, the technical means to launch attacks on the network are becoming more sophisticated, although at this stage, there are different intrusion prevention technology models to deal with. However, for unknown attacks, the existing intrusion prevention solutions cannot completely solve these unknown network attacks, and there is no "one size fits all" intrusion prevention model to solve all kinds of unknown network attacks [13]. In this context, active defense technology is gradually gaining great attention. It does not depend on the characteristics of the attack code and attack behavior but rather on the technical means of providing the operating environment, changing the static and deterministic nature of the system, to minimize the successful utilization of vulnerabilities, disrupt the implementation ability of network vulnerability exploitation, and block or interfere with the accessibility of the attack, thus significantly increasing the difficulty and cost of the attack [14]. Although the idea of active defense has been around for a long time, as an attack defense concept, there is still no standardized definition to date. A summary based on relevant literature is broadly divided into security defense models and active defense techniques [15].

3. Data-Driven WSN Security Threat Analysis Model Construction Based on Cognitive Computing

3.1. Cognitive Computing Model Design. Due to the limited computing resources and long-term operation of the IoT sensing device nodes aggregated and accessed by the edge computing terminals, the traditional "patch" security hardening mechanism cannot be applied to the IoT sensing device nodes, and the risk of malicious exploitation of the IoT sensing device nodes in uncontrolled environments is extremely high, which makes the edge computing terminals extremely easy to become the target or springboard of the IoT sensing device nodes. Therefore, how to effectively conduct the active defense of edge computing endpoints and detect and defend remote penetration attacks from IoT sensing device nodes in advance is often the first step in edge computing network security protection [16]. To address this, several terminal defense techniques have been proposed in related research, and the main implementation idea of these techniques is to use digital certificate authentication technology and trusted access technology to evaluate and authenticate the identity legitimacy, software and hardware integrity, and security of terminal entities, and only terminals that satisfy the access control policy specified by the system are allowed to access the network. However, with the continuous changes in the means of attack, malicious attacks are becoming increasingly covert; on the one hand, the terminal identity execution authentication and identification technology has been easily forged or bypassed; on the other hand, the legitimate terminal after welcoming the identity authentication is used as a springboard, so that the implementation of penetration attacks is difficult to be detected and identified.

Based on the idea of mimetic defense, a mimetic defense model for edge computing terminals is established based on the dynamic heterogeneous redundancy characteristics of the network attack chain and the mimetic defense system, and the possibility of successful attacks on each key component in the mimetic defense model can be solved based on this model, so that different parameters can be used to analyze the security defense effectiveness of the mimetic defense model for edge computing terminals, facilitating a better insight into how to use mimetic defense techniques designed to improve the security of edge computing endpoints. Figure 1 illustrates the relevant components studied in this chapter. As the network security situation becomes more complex, the technical means to launch attacks on the network are increasingly emerging, although at this stage, there are different intrusion prevention technology models to deal with. However, for unknown attacks, the existing intrusion prevention solutions cannot completely solve these unknown network attacks. At present, there is no "one size fits all" intrusion prevention model to solve all kinds of unknown network attacks. In this context, active defense technology has gradually gained people's attention.

The active defense model constructed based on the idea of mimetic defense is an IPO model; when the submitted request input enters the system, it is copied into n copies by the input agent unit and forwarded to the set of executors, which contains n similar redundant executors (k_1, k_2, k_3, …, k_m). By taking advantage of the dependency of cyberattacks on the environment, one attack against a specific vulnerability cannot be effectively played in heterogeneous executors (k_1, k_2, k_3, …, k_m) at the same time, thus achieving the defense effect against vulnerability attacks. The multiredundancy voter mainly compares the execution results of redundant executors in terms of discrepancy, to vote whether the mimetic defense system suffers from network intrusion and achieves the purpose of intrusion detection [17]. At present, the mimetic defense technology has formed a variety of systems with mimetic defense structure routers.

A cluster analysis algorithm is a statistical analysis method that can be used to deal with sample classification problems. It is based on similarity and does not require sample labeling. The cluster analysis algorithm tries to discover the implied relationships between different data in the sample space and classify the data into different groups by calculating the similarity between the data, which are more similar within the groups and less similar between the groups. The clustering algorithm is a very important and commonly used data mining algorithm in machine learning, which does not require prior knowledge of the characteristics of the sample categories which can be very good at discovering "unknown" relationships from "known" data. The clustering algorithm puts similar samples together in one category by calculating the similarity. The clustering analysis algorithm has the characteristics of clear computational logic and good sample classification.

The calculation of vector distances in competitive neural network algorithms usually uses the Euclidean distance method or the cosine method. The Euclidean distance method calculates the distances between vectors with the following formula:

$$\|X + X_i\| = \sqrt{(X_i - X)} - \sqrt{(X - X_i)}^T. \quad (1)$$

The algorithm to implement the "winner takes all" competition mechanism in competitive neural networks is as follows.

(1) Vector normalization

Vectors with different angles and lengths or too much difference will increase the computational complexity of the algorithm. Therefore, the vector is normalized to a unit vector with direction and length of 1.

(2) Finding the winning neuron

After the competing layer neurons acquire the sample objects in the input layer, the weights of all competing layer neurons are calculated for similarity with the input objects, and the competing layer neuron with the greatest similarity receives the highest weight to become the winning neuron.

(3) Adjustment of weights

Weights are adjusted for the winning neuron and wait for the next input. Competitive neural networks can arrive at the final winning neuron through the competition rule, but if the initial value of a neuron deviates from all samples to a large extent, then these neurons will still not be able to obtain a higher weight in the process of weight adjustment for as long as they are trained, and as a result, these neurons

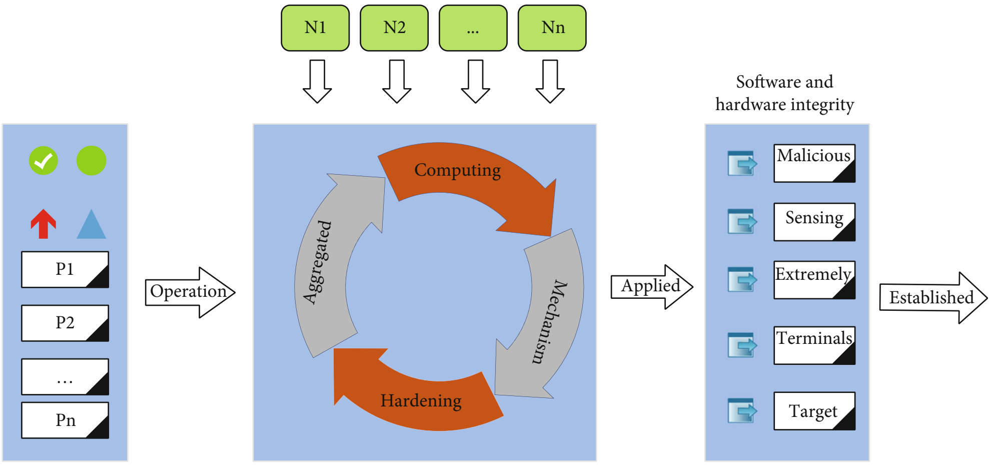

Figure 1: Framework of remote access anti-infiltration technology for computing endpoints.

will never win and will naturally not be activated. Such inactivated neurons are called "dead neurons." The problem of dead neurons is solved by adding a threshold learning rule to the weight adjustment rule of the competing layer neurons of the competitive neural network [18]. The threshold learning rule sets a higher threshold for neurons with a low probability of winning to improve the competitive ability of the neuron and a smaller threshold for neurons that win frequently to make each neuron likely to win. Finally, the average degree of neuron weight adjustment is calculated to output the final winning neuron.

$$P_1 = \frac{3}{\beta_2}\left(P' + \beta_1 p_2\right). \tag{2}$$

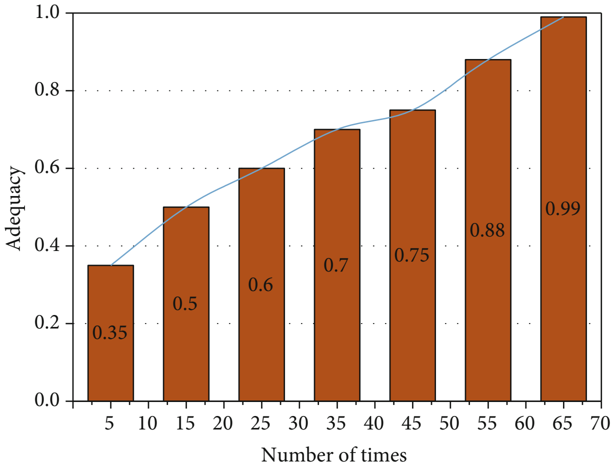

Figure 2: Relationship between the number of interactions and adequacy.

After taking the direct trust value, the weight of the direct trust value is then calculated. The weight of the direct trust value is used to indicate the reliability of the direct trust value, and its value is related to the dispersion of the historical interaction trust value and the adequacy of the historical interaction. The relationship between the number of interactions and the sufficiency is shown in Figure 2. When the number of interactions N is 30, the interaction sufficiency reaches 95%, and when the number of interactions reaches 50, the sufficiency is almost close to 100%. Clustering analysis algorithms are very important and commonly used data mining algorithms in machine learning. They do not need to know the characteristics of sample categories in advance and can find "unknown" relationships from "known" data. The clustering algorithm puts similar samples together into one category through the calculation of similarity. The cluster analysis algorithm has the characteristics of clear calculation logic and good sample classification effect.

The weight formula can be expressed as shown in equation (3). This setting enables the weight of the direct trust value to be inversely proportional to std and positively proportional to freq, where $\varpi_{ji}^{\mathrm{DT}}$ denotes the direct trust weight of the node numbered j to the node numbered i. Multiplying by 1/2 is to normalize the weights between 0 and 1. Up to this point, the direct trust value and direct trust weight are calculated and the whole direct trust module has been designed.

$$\varpi_{ij}^{\mathrm{TD}} = 2(\mathrm{freq} + \mathrm{std} - 1). \tag{3}$$

3.2. WSN Security Threat Analysis Model Construction. The Internet of Things (IoT) is a fusion of automation systems and IoT systems, which features comprehensive sensing, interconnected transmission, intelligent processing, intelligent handling, and self-organization and maintenance, and its applications span many fields such as intelligent transportation, smart factories, smart grids, and intelligent environmental detection [19]. The IoT can be viewed as a subset of the IoT and can be structurally divided into three layers: data collection layer, data transmission layer, and data processing layer. The security of the entire network relies on this certification center, and the certification center is easily identified by malicious nodes and is attacked, which poses great security risks; when the network is large and the performance of the certification center is limited, the

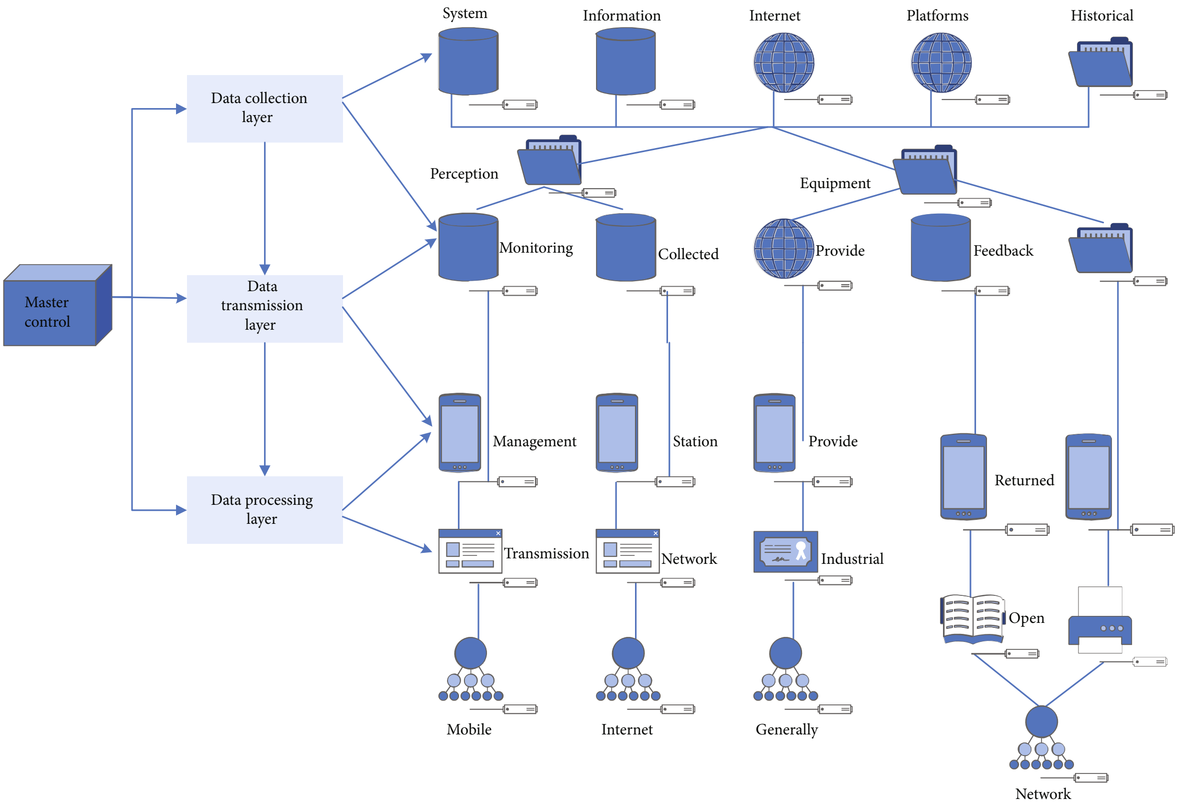

Figure 3: IoT system architecture.

network may collapse at any time. A typical system architecture for a wireless network is shown in Figure 3.

The blockchain infrastructure has six main layers, each layer completes a part of the core tasks, and the layers collaborate to achieve a decentralized trust model; from bottom to top, there are mainly data layers, network layers, consensus layers, incentive layers, contract layer, and service layer. The data layer represents the physical form of the blockchain technology and is the basic technical structure for designing the blockchain ledger, describing which parts the blockchain consists of. Each block contains many technologies, such as timestamp technology and hash cryptography function, which is used to ensure that the blocks are connected in sequential order and that the data saved in the blockchain is not tampered with; the main function of the network layer is to enable communication between the nodes in the blockchain network and to achieve a distributed record of information [19]. The purpose of the blockchain network is to create a P2P (peer-to-peer network) to solve the problem of single-point congestion and failure in traditional networks, where each node is both a sender and a receiver of messages; the knowledge layer is responsible for efficiently reaching a consensus on a certain aspect in a decentralized system through information exchange between highly decentralized and distrustful nodes, which is the core idea of blockchain. Commonly used consensus algorithms are the proof-of-workload algorithm, proof-of-share authorization algorithm, practical Byzantine fault tolerance algorithm, etc. Cognitive computing is based on mathematical methods, based on computer technology, and guided by the results of bioneurology to realize the analysis of data by simulating the mechanism of the human brain. The application of cognitive computing to mine the value of data will help people discover potential patterns and improve working methods.

$$y^2 + bx - ay^2 \leq x^2 + cy^3 - dx + e. \tag{4}$$

Hashing is a method of applying a hash function to data that maps an input of any size (file, text, or image) into a fixed-length binary value. The hashed hash value is very different if the original information is slightly modified, so hash functions are commonly used in blockchains to verify the integrity and accuracy of data.

Hash functions have several important security properties as follows:

(1) They are reverse resistant. This means that they are one-way irreversible, and computing the correct input value given some output value does not work here with hash functions. For example, given digest, finding hash $(x) =$ digest is infeasible

(2) They have a second inverse. This means that it is impossible to design a hash function to find a second input that produces the same output by giving a particular input

The latter block in the blockchain holds the hash value of the previous block to form a chain structure, and once the data in the previous block changes, the hash pointer in the block header of the latter block will follow, so it is difficult to tamper with the data in the blockchain. The Internet of Things is the integration of automation systems and Internet of Things systems. It has the characteristics of comprehensive perception, interconnected transmission, intelligent processing, intelligent processing, and self-organization and maintenance. Its applications are widespread in intelligent transportation, smart factories, smart grids, smart environment detection, etc. In the field, the Internet of Things can be regarded as a subset of the Internet of Things.

As symmetric encryption is difficult to solve the key management and digital signature problems, asymmetric encryption was born. In the process of asymmetric encryption, X represents the plaintext, which indicates the input of the algorithm; the public key used for encryption and the private key used for decryption are different; Y is the ciphertext, which indicates the data obtained after encryption. The steps of the public key cryptosystem are shown below [20].

The encryption algorithm gets the encrypted ciphertext based on the input plaintext and the public key, which is delivered to the destination through the network, and the receiver decrypts the received ciphertext with the private key to get the same plaintext as the one sent by the sender. This completes the entire process of asymmetric encryption. The most widely used asymmetric encryption regimes are the RSA algorithm, ElGamal algorithm, etc. The advantages of the asymmetric encryption system are as follows: unlike symmetric encryption, the sender and the receiver need to share the same password and each has its key, eliminating the link of transmitting the key and reducing the security risks in the network; even if the public key is intercepted by the attacker in the process of transmission, the ciphertext cannot be decrypted even if the public key is obtained because there is no private key matching the public key, ensuring that the n users only need n pairs of keys, which is easy to manage as the key distribution is simple, and only need to distribute the encryption key to each other and keep the decryption key by themselves. But the disadvantage is that the encryption algorithm is complex and the encryption and decryption speed is slow.

$$3a^4 + 15b^2 \leq 0. \tag{5}$$

Wireless sensor networks have many sensor nodes and large network sizes and are usually deployed in exposed external environments, making them vulnerable to various forms of attacks. Distributed authentication by establishing a trust model can effectively reduce attacks. The node trust mechanism is the basis of the trust model. Wireless sensor networks are mainly used to transmit data information through mutual aid forwarding between nodes, and establishing trust mechanisms between nodes can effectively resist malicious attacks. In the network, nodes choose whether to interact with the target node by judging its trustworthiness.

There are many and dense nodes in WSNs with large network sizes; due to the low cost of sensors, the computational capacity, storage capacity, and power supply are limited; it is difficult to perform authentication and cannot guarantee network security. Establishing an authentication model can effectively solve this security problem. The authentication model is divided into centralized authentication and distributed authentication, and the centralized authentication mechanism has many drawbacks: the network structure is simple and not strong against attacks, the network scalability is poor, the performance of the authentication center is limited, and the network will collapse at any time when the network scale is expanded; therefore, the security of centralized authentication is not high. Therefore, this section also focuses on the principle and current research status of distributed authentication models and compares the existing models with the RRCTM model proposed in this paper.

4. Analysis of Results

4.1. Cognitive Computing Model Results. For some samples that can be identified by the "naked eye" based on experience and criteria, the number of classifications can be identified. The K-DB algorithm is chosen to not only determine the radius and density thresholds more accurately but also to identify core, boundary, and outlier points in the sample. The analysis based on the analysis of sample points of different nature can make the study of the sample more comprehensive and targeted. The core points with the smallest average distance in the density clustering results can be used to characterize the nearest similar objects of all samples of the cluster, which to some extent reflects the overall characteristics of the cluster [21]. The boundary points in the clustering results are used to characterize the farthest similar objects of all samples in the cluster and are suitable for judging the extreme attributes and characteristics of the cluster; outliers can be used to determine the reason for the occurrence of the sample and analyze the problems in the data information; in practical applications, outliers can be dealt with, or they can be selectively discarded. The boundary points in the clustering results are used to characterize the farthest similar objects of all samples of the cluster, which are applicable to determine the extreme properties and characteristics of the cluster; outlier points can be used to determine the reasons for the appearance of the sample and analyze the problems in the data information, and the outlier points can be processed or selectively discarded in practical applications.

Cluster quality assessment methods use the Cluster Validity Index (CVI) to assess the effectiveness of clustering. Cluster quality assessment is commonly performed by internal, external, and expert evaluation. The internal evaluation assesses the effectiveness of clustering by obtaining assessment quality scores according to calculation rules. When a node is subject to intermittent attacks or random errors, the reputation value of the node will decrease. This type of node is an abnormal node, but due to the low frequency of attacks or errors, it does not affect the normal communication of the node. The reputation value of the node is also maintained above 0.8. External assessment is a controlled assessment using public standards, and expert assessment is a manual assessment method that indirectly assesses the effect of clustering through expert knowledge. This experiment uses internal evaluation to verify the effectiveness of the K-DB algorithm. The circle blob dataset contains 6000 data items, which can be roughly divided into 3 clusters according to the sample distribution, and the DBSCAN algorithm adjusts the density threshold Mats to 40 after the 4th iteration to obtain better clustering results. The clustering results of the density clustering algorithm with a density radius of 0.13 and a density threshold of 60 are calculated according to the K-DB algorithm in Figure 4.

To further verify the superiority of the K-DB algorithm, this paper selects real datasets from the UCI database for experimental validation of algorithm accuracy and efficiency. The experiments are compared with K-means, DBSCAN, and K-DB algorithms on the real datasets Iris, Wine, and Glass, and this experiment uses the Davidson-Fortin Index (DBI) and accuracy (ACC) to compare and validate the performance of the K-DB algorithm. The experimental results are shown in Table 1.

From the table, the K-DB algorithm outperforms K-means and DBSCAN algorithms in terms of clustering accuracy on all three real datasets, and the K-DB algorithm effectively improves the accuracy of density radius and threshold setting. The K-DB algorithm combines the advantages of the two algorithms to achieve complementary advantages and has higher accuracy and a smaller DBI than the single K-means and DBSCAN algorithm. Experimental results show that the K-DB algorithm has superiority in improving algorithm efficiency and clustering accuracy and can identify core points, boundary points, and outliers in sample clusters. The K-DB algorithm combines the advantages of both algorithms to achieve complementary strengths and has higher accuracy and smaller DBI than single K-means and DBSCAN algorithms. The experimental results show that the K-DB algorithm is more accurate than the single K-means and DBSCAN algorithms. The experimental results show that the K-DB algorithm is superior in improving the efficiency and clustering accuracy of the algorithm and can identify core points, boundary points, and outliers in the sample clusters.

$$a_{ij} = p\left(q_{j-i} = \mathrm{IS}_i\right), \sum_{i=1}^{m} a_{ij} = 1. \tag{6}$$

To predict the security reliability of all the reachable paths in the network topology mimetic association graph, this paper classifies the network security reliability hidden state level into 5 values. The reliability of each reachable path will be transferred with probability among these 5 states. The observation sequence $O = \{o_1, o_2, L, o_3\}$ is obtained after t moments of observation. For example, for the network throatiness metric, the observation sequence is the network anomaly measure obtained after t moments. From the HMM definition, it is known that a total of 2 posture prediction models for 2 observable metrics need to be constructed and integrated into four steps to determine the network security reliability transfer probability at the next moment.

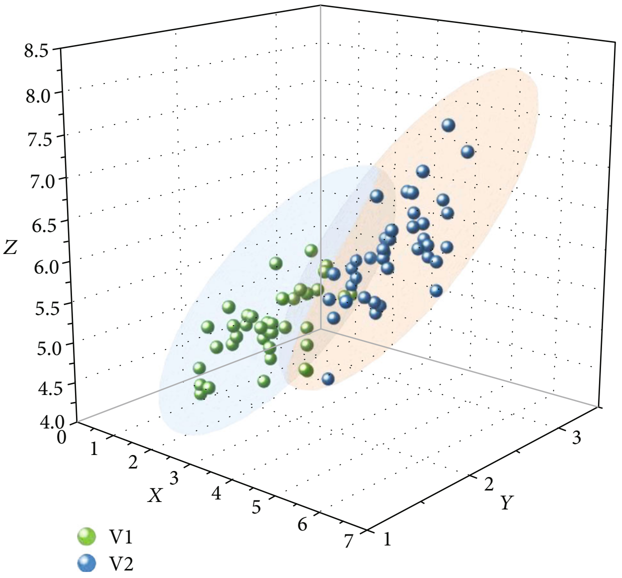

Figure 4: K-DB clustering data distribution for the circle blob dataset.

Table 1: Accuracy of clustering results for real datasets.

	K-D		K-E		K-F		K-G	
	ab	ce	ab	ce	ab	ce	ab	ce
UCI	0.92	3.53	0.821	3.62	0.786	3.89	0.694	2.94
DBSCAN	0.83	3.15	0.795	3.54	0.754	3.75	0.678	2.84
K-DB	0.76	2.71	0.734	3.41	0.722	3.61	0.662	2.74
ACC	0.71	3.21	0.756	3.45	0.696	3.47	0.646	2.64
GLASS	0.65	2.92	0.712	3.67	0.658	3.33	0.635	2.54

4.2. *WSM Security Threat Analysis Model Simulation Experiment.*

To facilitate the modeling, the following assumptions are made in this paper related to the network model properties of wireless sensor networks.

(a) All nodes deployed in the monitoring area are statically deployed, and the node locations can be moved at will

(b) Each node has a unique network-wide identification ID, and its residual energy and geographic coordinates are sensed

(c) All nonbase station nodes have the same energy at the initial moment, and the energy cannot be replenished

(d) Each node has the same storage, computing, and communication capabilities except for the base station

(e) The sensor nodes can dynamically adjust the node transmit power to accommodate different communication distance requirements

WSN is characterized by many sensor nodes and large network scale. It is usually deployed in an exposed external environment, so it is vulnerable to various forms of attacks. Authentication is the basis for ensuring network security. Traditional authentication mostly uses centralized authentication. Since the research proposal in this paper focuses on the hierarchical security model, a simple energy consumption model involving only communication is used here and does not consider the energy consumption of the nodes in the process of computing and storing data. The energy consumption of the node sending data is divided into two parts: RF transmitting consumption and signal amplifier consumption; the energy consumption of the node receiving data is only the consumption of the receiving circuit. Security is an important metric to evaluate the merits of a defense method, and this section analyzes the resistance to attacks of the proposed edge computing network attack active defense technique based on network topology mimetic correlation.

The attack method is a SYN flood for guided DoS attacks, and the average service response time of the network topology mimetic correlation system is tested under different SYN flood attack rates to reflect the service availability performance. Figure 5 shows the results showing that the network topology mimetic association strategy proposed in this paper can better resist DoS attacks because the network topology mimetic association technique dynamically measures network anomalies for the strength of network attacks and performs automatic adjustment of the network topology mimetic association graph and communication paths, which increases the path hitting difficulty of DDoS attacks. This is because when the network topology mimetic association graph space is squeezed to almost zero, the DDoS attack enters an unguided blind attack state; i.e., the attacker detects all nodes in the reachable paths and attacks them on average.

A comparison of the change in reputation value of different types of nodes in the network under the condition that no management node rotation is performed showed that the reputation value of normal nodes that are not under attack does not change significantly throughout the cycle and the node reputation value remains normal. When a node is subjected to intermittent attacks or random errors, the reputation value of the node decreases and this type of node is an abnormal node, but due to the low frequency of attacks or errors, it does not affect the normal communication of the node, and the reputation value of the node is maintained above 0.8. The security of the network completely relies on the certification center. Once the certification center is maliciously attacked, the entire certification system will collapse; when the network scale is expanded, the computing power and storage capacity of the certification center will be limited, which will affect the performance of the network; with the development of WSN, the topology of the network is ever-changing, and the flexibility of centralized authentication is not enough. When the node is under continuous uninterrupted attacks, after about 50 s, the node reputation value starts to drop exponentially and rapidly to below the threshold value of 0.2 and the node is cut out of the network.

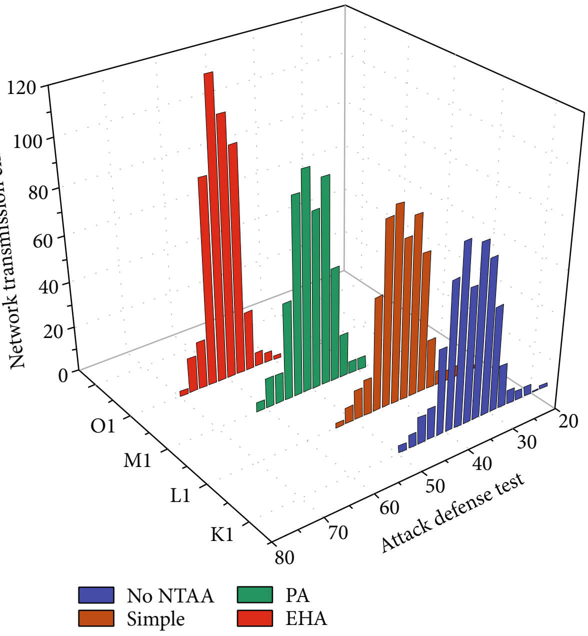

Figure 5: DOS attack defense test results.

In this section, with the help of TOSSM, a simulation tool for WSNs, the physical and link layer protocols of IEEE 802.15.4 are used and ACK/NACK is disabled to experimentally evaluate and compare the transmission performance of GCCT with existing typical protocols such as CTPII and SHMT0. The wireless channel uses a random erasure channel; i.e., the MAC layer discards the received packets with a certain probability, thereby generating Bernoulli-distributed packet loss. Simulation results (averaged over 100 simulations) are given below for end-to-end single data stream communication and many-to-one aggregated data stream communication, respectively.

For single-stream communication, the protocol performance is evaluated here in terms of 3 aspects: packet loss rate, node density, and transmission hops, where node density refers to the average number of neighboring nodes of the nodes in the network. Three metrics are used to evaluate the algorithm performance: (a) packet delivery success rate, i.e., the percentage of packets successfully received by the sink node from the source node; (b) transmission delay, i.e., the time used for packets to be received from the source node to the sink time; and (c) communication overhead, i.e., the total number of packets sent by the network nodes during transmission. In terms of energy balance, the first two schemes have some advantages and the number of nodes that die in the early stage is less; although Figure 6 shows that at 500 s the SCM scheme still has close to 100 nodes surviving, the experimental results show that due to the high energy consumption of the nodes in the early stage, most of the nodes are on the verge of death and at 530 s the nodes all die. In terms of node

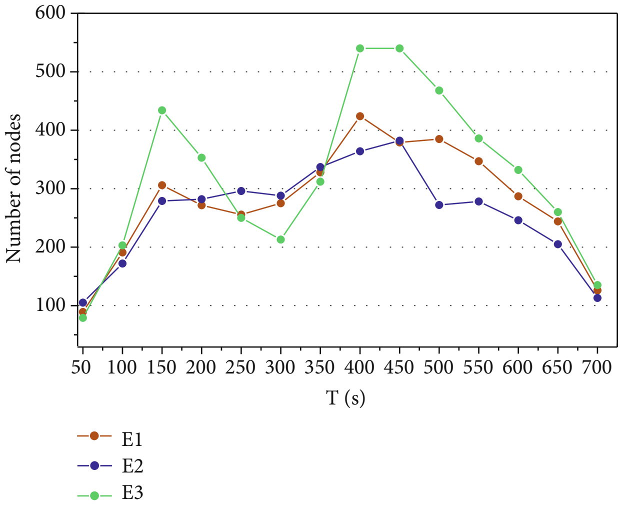

Figure 6: Comparison of the number of nodes surviving at different points in time.

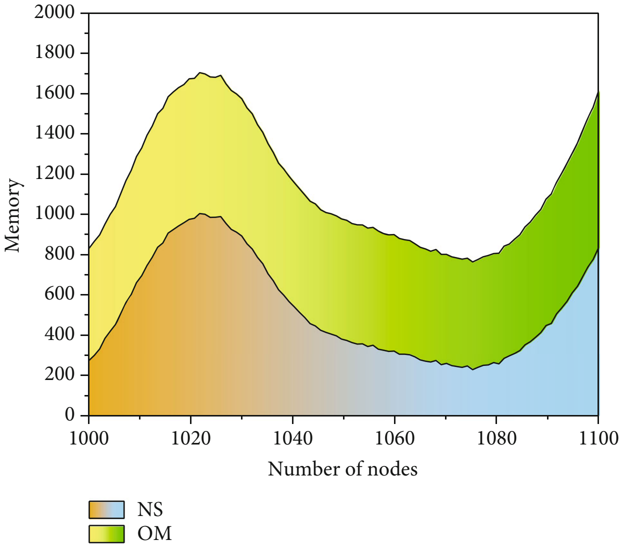

Figure 7: Simulation performance comparison.

survival time, the survival of nodes in this model is better than the first two scenarios in the later stage.

The comparison of the total energy consumed by the network with a capacity of 400 nodes over time shows that the initial energy of a single node in the network is set to 2 J and the total energy of the nodes in the network is 800 J. The comparison of this method with the SCM scheme and the improved LEACH protocol shows that the total energy consumed by the nodes in this model is significantly lower in 500 s of survival time. In terms of the remaining energy, the node energy in the SCM and LEACH schemes is depleted, while the total energy of the network in this model is about 25% remaining, mainly since the cluster head election is performed inside the subnet in this model, which reduces the energy consumption of communication with nodes at longer distances. The energy-saving effect will be more significant for wireless sensor networks deployed over large areas. The data collection unit is responsible for collecting and converting the information in the monitoring area; the data transmission unit mainly sends and receives the collected data information in the form of wireless communication. To establish a wireless sensor network environment, many sensors, a data transmission center, and a base station are required.

Under the same conditions, the performance of the two simulation platforms is compared mainly by their memory consumption through experiments with the improved LEACH protocol on NS-3 and WSPSim based on OMNeT++, and the performance comparison is shown in Figure 7. Therefore, this system is more advantageous for large-scale WSN.

This section improves the classical LEACH protocol by adding an MD5 hash encryption mechanism and trust evaluation mechanism, which is modeled and simulated by the functional modules already developed in this simulation platform. The simulation results are compared to verify the correctness of the module and the security of the improved protocol and verify that through simulation experiments, this platform can correctly simulate WSN-related protocols and algorithms and has good adaptiveness and ease of use compared to other simulation platforms.

5. Conclusion

The security of wireless sensor networks as an important carrier in the future era of the Internet of everything is becoming more prominent, and maintaining the security of wireless sensor networks is as important as human beings protecting their nervous system. By dividing the modules through a clustering analysis algorithm, the intelligent mechanism of “functional separation” of the cerebral cortex is introduced into the practice of a single neural network to solve the problems of oversized structure, high computational complexity, and weak interpretation in neural network problem processing engineering. A modular neural network-based feature combination recommendation model is designed to achieve the extraction of important features from sample data and help people make fast and accurate decisions. The experimental results show that the computational overhead of the RRCTM model is significantly reduced, and the RRCTM model is more accurate for the evaluation of trust values and has strong dynamic adaptivity and high sensitivity, which can effectively resist various malicious node attacks and ensure the security of wireless sensor networks. Some progress has been made in this research work, but there are still some security issues that need further research. The current studies have focused on the security of over-the-air data distribution based on network-coded data distribution protocols, neglecting the security management of the code image after it is received by the sensor nodes. If the new code image is an update about a military application code, its content is sensitive and special treatment of the code image is required to secure it. Thus, security mechanisms for the storage, use, and destruction of code images on sensor nodes will be investigated in the future.

Data Availability

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

Conflicts of Interest

The author declares that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by Shandong University of Finance and Economics.

References

[1] D. Sivaganesan, "A data driven trust mechanism based on blockchain in IoT sensor networks for detection and mitigation of attacks," *Journal of Trends in Computer Science and Smart Technology*, vol. 3, no. 1, pp. 59–69, 2021.

[2] A. Williams, P. Suler, and J. Vrbka, "Business process optimization, cognitive decision-making algorithms, and artificial intelligence data-driven internet of things systems in sustainable smart manufacturing," *Journal of Self-Governance and Management Economics*, vol. 8, no. 4, pp. 39–48, 2020.

[3] M. S. Munir, S. F. Abedin, N. H. Tran, and C. S. Hong, "When edge computing meets microgrid: a deep reinforcement learning approach," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7360–7374, 2019.

[4] A. Clark, "Big data-driven transportation planning and engineering: smart urbanism, autonomous vehicle algorithms, and network connectivity systems," *Contemporary Readings in Law and Social Justice*, vol. 12, no. 2, pp. 70–78, 2020.

[5] M. Mahmud, M. S. Kaiser, M. M. Rahman et al., "A brain-inspired trust management model to assure security in a cloud based IoT framework for neuroscience applications," *Cognitive Computation*, vol. 10, no. 5, pp. 864–873, 2018.

[6] S. Tripathi and S. De, "Data-driven optimizations in IoT: a new frontier of challenges and opportunities," *CSI Transactions on ICT*, vol. 7, no. 1, pp. 35–43, 2019.

[7] D. Watkins, "Real-time big data analytics, smart industrial value creation, and robotic wireless sensor networks in Internet of things-based decision support systems," *Economics, Management, and Financial Markets*, vol. 16, no. 1, pp. 31–41, 2021.

[8] W. Xu, Y. Xu, C. H. Lee, Z. Feng, P. Zhang, and J. Lin, "Data-cognition-empowered intelligent wireless networks: data, utilities, cognition brain, and architecture," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 56–63, 2018.

[9] C. Morgan, "Can smart cities be environmentally sustainable? Urban big data analytics and the citizen-driven Internet of things," *Geopolitics, History, and International Relations*, vol. 12, no. 1, pp. 80–86, 2020.

[10] F. Shi, H. Ning, W. Huangfu et al., "Recent progress on the convergence of the Internet of things and artificial intelligence," *IEEE Network*, vol. 34, no. 5, pp. 8–15, 2020.

[11] I. Yaqoob, K. Salah, M. Uddin, R. Jayaraman, M. Omar, and M. Imran, "Blockchain for digital twins: recent advances and future research challenges," *IEEE Network*, vol. 34, no. 5, pp. 290–298, 2020.

[12] B. Hyman, Z. Alisha, and S. Gordon, "Secure controls for smart cities; applications in intelligent transportation systems and smart buildings," *International Journal of Science and Engineering Applications*, vol. 8, no. 6, pp. 167–171, 2019.

[13] Y. J. Qu, X. G. Ming, Z. W. Liu, X. Y. Zhang, and Z. T. Hou, "Smart manufacturing systems: state of the art and future trends," *The International Journal of Advanced Manufacturing Technology*, vol. 103, no. 9-12, pp. 3751–3768, 2019.

[14] A. Toma, A. Krayani, M. Farrukh et al., "AI-based abnormality detection at the PHY-layer of cognitive radio by learning generative models," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 1, pp. 21–34, 2020.

[15] L. Yang, W. Li, M. Ghandehari, and G. Fortino, "People-centric cognitive Internet of things for the quantitative analysis of environmental exposure," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2353–2366, 2018.

[16] M. M. Hussain, M. S. Alam, and M. M. S. Beg, "Fog computing model for evolving smart transportation applications," *Fog and Edge Computing: Principles and Paradigms*, vol. 22, no. 4, pp. 347–372, 2019.

[17] F. Kong and Y. Wang, "Multimodal interface interaction design model based on dynamic augmented reality," *Multimedia Tools and Applications*, vol. 78, no. 4, pp. 4623–4653, 2019.

[18] Y. Liu, X. Ma, L. Shu, G. P. Hancke, and A. M. Abu-Mahfouz, "From Industry 4.0 to Agriculture 4.0: current status, enabling technologies, and research challenges," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4322–4334, 2021.

[19] W. Shi, W. N. Chen, Y. Lin, T. Gu, S. Kwong, and J. Zhang, "An adaptive estimation of distribution algorithm for multipolicy insurance investment planning," *IEEE Transactions on Evolutionary Computation*, vol. 23, no. 1, pp. 1–14, 2019.

[20] J. Keane, "Can self-driving cars lead to sustainability? Autonomous smart sensors, perception and planning algorithms, and data processing efficiency," *Contemporary Readings in Law and Social Justice*, vol. 12, no. 1, pp. 9–15, 2020.

[21] C. Zhou, B. Hu, Y. Shi, Y. C. Tian, X. Li, and Y. Zhao, "A unified architectural approach for cyberattack-resilient industrial control systems," *Proceedings of the IEEE*, vol. 109, no. 4, pp. 517–541, 2021.