frontiers | Frontiers in Energy Research

TYPE Original Research
PUBLISHED 07 February 2023
DOI 10.3389/fenrg.2023.1113384

OPEN ACCESS

EDITED BY
Praveen Kumar Donta,
Vienna University of Technology, Austria

REVIEWED BY
Vinit Gunjan,
CMR Institute of Technology, India
William Tichaona Vambe,
Walter Sisulu University, South Africa

*CORRESPONDENCE
Jianfei Chen,
jianghai166@163.com

This article was submitted to Smart Grids, a section of the journal Frontiers in Energy Research

RECEIVED 01 December 2022
ACCEPTED 11 January 2023
PUBLISHED 07 February 2023

CITATION
Chen J, Zhao L, Sun Q and Zhang C (2023), Security feedback trust model of power network demand response terminal triggered by hacker attacks.
Front. Energy Res. 11:1113384.
doi: 10.3389/fenrg.2023.1113384

Security feedback trust model of power network demand response terminal triggered by hacker attacks

Jianfei Chen[1]*, Lina Zhao[2], Qiang Sun[3] and Cheng Zhang[4]

[1]State Grid Shandong Electric Power Company, Jinan, China, [2]Information and Communications Company, State Grid Shandong Electric Power Company, Jinan, China, [3]State Grid Weihai Wendeng Power Supply Company, Weihai, China, [4]State Grid Juxian Power Supply Company, Rizhao, China

With the rapid expansion of power system scale, demand response business is promoted to develop. More and more demand response terminals are connected to the smart grid, smart grid is an intelligent system that allows the grid to effectively perform its functions. Its data can be used in intelligent decision-making during grid operation, which may be attacked by hackers in practical applications, causing security problems of demand response terminals of the power network. The security feedback trust model establishes trust relationship through trust mechanism, which can effectively ensure the security of interaction between nodes and demand response terminals of the smart grid. Therefore, a security feedback trust model of power network demand response terminal triggered by hacker attacks is proposed. Analyze the role of smart grid in power grid, and use convolutional neural network in artificial intelligence technology to enhance the flexibility of smart grid. Aiming at the security problem of the demand response terminal of the power network being attacked by hackers, based on the trust theory, the security feedback trust model of the demand response terminal of the power network is designed through the main services provided by the security feedback trust model, the trust information storage of the power network nodes and the summary of the main work. Establish the identity trust relationship, adopt the distributed verifiable signature scheme, update the power grid node certificate, update the identity trust relationship, and revoke the identity trust relationship based on the trust evaluation and threshold value to prevent hackers from attacking the power grid demand response terminal. Based on information theory, trust is established and measured. Entropy is used to represent the trust value. Behavior trust evaluation and composition mechanism are introduced into the security feedback trust model of power network demand response terminals to achieve the credibility of identity and behavior among power network nodes. The experimental results show that the proposed method can judge the hacker attacks, reduce the impact of hacker attacks on the trust of power grid nodes, and improve the interaction security between power grid demand response terminals and power grid nodes.

KEYWORDS

hacker attacks, power network, trust assessment, node certificate, demand response terminal, security feedback trust model, artificial intelligence, smart grid

1 Introduction

At present, the energy revolution is further integrated with the digital revolution, vigorously promoting the innovative development of the energy industry and the Internet. The power system is an important part of the energy network. With the continuous improvement of the intelligent degree of the power system, the coupling degree between the power network and the information network is constantly improving. They are interdependent and interact with each other. The normal operation of the information network cannot be separated from the power support of the power network. The switching and adjustment operations of each node in the power network need to be realized through the information network (Li et al., 2021a; Zhang et al., 2021a; Sun et al., 2022). Considering that the demand for interactive regulation responds to the increase in the number of service deployed terminals, which is different from the previous terminals, which are mostly accessed by dedicated lines or deployed sporadically through pilot projects. Without the security test of the external network, a large number of demand response terminals are connected to the power network. At the same time, according to the protection requirements, the data, and control information transmitted by the terminal connected to the power network are blurred in the horizontal isolation boundary of the security zone, which may be attacked by hackers in practical applications, resulting in a large area of power failure and interruption of communication between devices. The security feedback trust model is to establish the trust prediction value of external entities through a reasonable trust system model, and correctly judge the trust degree of the other entity, so as to promote the safe, high-speed and harmonious development of the entire power network demand response terminal, which can effectively solve the security problems of the power network demand response terminal attacked by hackers (Jiang et al., 2019; Liu et al., 2020). Therefore, it is of great significance to establish the security feedback trust model of power network demand response terminal.

At present, scholars in related fields have studied the power trust model. Zhang et al. (2019a) proposed a master-slave chain architecture model for cross domain trusted authentication of power services. With the gradual complexity of China's electricity information, the current power business is diversified, and multi business integration is increasingly becoming the direction of power business development. However, the integration of commercial trust and mutual trust has not been effectively solved, which will bring huge economic losses to the power grid. Therefore, while effectively isolating multiple services, how to ensure the integration and reliability of multiple services is an urgent security issue. This paper introduces a master-slave chain architecture based on blockchain, which is used for cross domain trusted authentication of power services. Use slave chains to isolate multiple services. The trunk ensures the trust of the business and minimizes the untrusted security risks. Alagappan et al. (2022) proposed a zero trust network architecture to enhance the security of virtual power plants. In order to prevent and contain network threats or network crimes, considering the ability of the architecture, a single damaged endpoint in a zero trust network is unlikely to spread horizontally, thus infecting the entire network. This provides the ability to adopt the architecture in the energy sector. The popularity of distributed generators enables consumers to supply power to the grid. These small generators form a virtual power plant. Through this arrangement, its network also faces security challenges and needs to protect these physical systems, data protection and information privacy. However, the above methods still have the problem of low security of power network demand response terminals. In order to establish the trust relationship between power grid nodes and improve the security of interaction between power grid nodes and demand response terminals, a comprehensive zero trust security architecture needs to be built to help power grid reduce system risk and protect data privacy under hacker attacks.

In order to improve the security of power network node interaction and demand response terminal, a security feedback trust model of power network demand response terminal triggered by hacker attacks is proposed. Based on the definition of trust theory, the security feedback trust model of power network demand response terminal is designed. By establishing, updating and revoking the identity trust relationship, the trust is established and measured based on information theory, and the trust value is expressed by entropy. The behavior trust evaluation and composition mechanism is introduced into the security feedback trust model of power network demand response terminals to achieve the identity trust and behavior trust between power network nodes. The security feedback trust model of power grid demand response terminal is constructed by trust theory, and the behavioral trust evaluation and synthesis mechanism are input into the model, can judge the hacker attacks, reduce the impact of hacker attacks on the trust of power grid nodes, and improve the interaction security between power grid demand response terminals and nodes.

2 Literature review

Cherukuri et al. (2022) designed Raspberry Pi to develop a family safety framework. After the intruder is identified, the intrusion detection system will pay attention to the image of the intruder. After the intrusion is identified, the mobile owner/administrator will be sent an alarm email with the recognizable and visible images of the attacker (facial view). The owner can also watch the real-time monitoring through the camera head on the intelligent device in the settings used to view the surrounding environment of the house.

Karthik et al. (2022a) uses visual encryption technology to hide original information such as images and texts. In VC, the basic principle is to segment the image and recreate it. According to the size, quality, pixel expansion, and nature of the image, the image is encrypted and improved to an 8-bit key.

Karthik et al. (2022b) used the deep transfer learning strategy to find network attacks in a simple way, and with the help of Analytics, collected information from IOT devices to be obtained. The nine current data sets of IOT are comprehensively tested, and the output results show that the proposed model significantly improves the accuracy of identifying IOT attacks.

Das and Mukherjee, (2022) analyzed the spying and security vulnerability cases that endanger user privacy and proposed blockchain technology. Blockchain distributed ledger is a new technology system, which can easily solve the security vulnerability problem with the help of the Internet of Things system. It can be used in energy, health, entrepreneurship, finance, and other fields. It has huge benefits and innovation potential.

Gunjan et al., (2014) studies data protection based on digital and cloud computing systems. Data protection is to build a data security

system covering the whole life cycle of data from the perspective of assets, intrusion and risk under the guidance of zero trust architecture. In order to improve the work efficiency more accurately, it requires not only technical expertise to crack it, but also to improve the security of users. Through this study, we will check the level of consciousness of cyber crime and security profession, and propose the necessary methods that really help to make the cyber environment safe, stable and credible.

Prasad et al., (2022) proposed a blockchain based medical image privacy access control mechanism and collaborative analysis. Image privacy refers to the process of protecting the information that involves individuals or organizations and should not be disclosed in the image during data collection, data storage, data query and analysis, and data distribution. Build a system model based on two stages of data cleaning and disease classification, write the model obtained after training into the blockchain, use the model with the best performance on the chain to identify the image quality when cleaning data, and transfer high-quality images to the disease classification model for use.

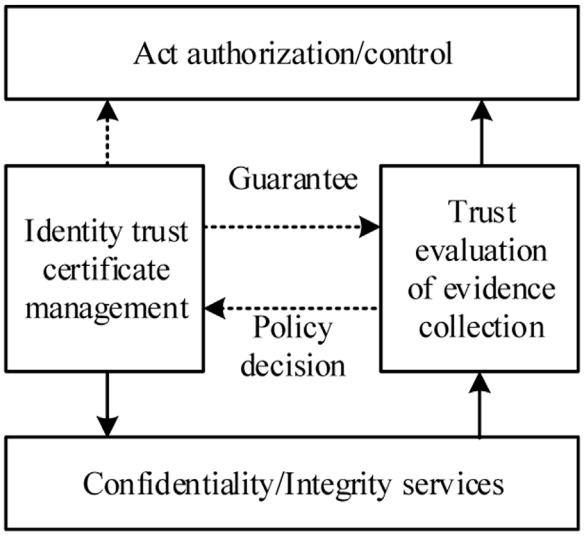

FIGURE 1
Overall structure of security feedback trust model of power network demand response terminal.

3 Security feedback trust model of power network demand response terminal

As the power network demand response terminal is connected to the external network, it may be attacked by hackers in the process of information transmission. Hacker attack is an unauthorized illegal access. The malicious acts of hackers attacking the internal nodes of the power grid will cause catastrophic damage to them (Wang et al., 2021; Group, 2022; Xu and Hong, 2022). It is mainly through the occupation of power network bandwidth, CPU, memory, and other resources, resulting in network performance degradation, or even failure, thus affecting the normal access of users. Therefore, establish a unified trust management model based on trust theory to form a formal description and measurement method of trust and privacy (Ren et al., 2020), improve the overall operation ability and anti attack ability of the power grid, then, the security feedback trust model of power network demand response terminal is designed.

3.1 Overall design of model

Convolution neural network is a feedforward neural network with convolution calculation and depth structure, which is one of the representative algorithms of depth learning (Li et al., 2021b; She et al., 2021). Convolutional neural network has the ability of representation learning. It can translate and classify the input information according to its hierarchical structure, and effectively identify hacker attacks in the power network.

The original members who participate in the establishment of a social group have the highest power and are called managers. New members need their approval to join, which is called general members. Managers can enjoy the benefits and services of members of other social groups preferentially. Under this incentive, each member works hard to serve the group to improve the trust of other members. Members who are unwilling to cooperate with other members will not be trusted by other members and will eventually be abandoned by the group. By referring to the level of trust, management members can develop general members into managers, or can exclude untrustworthy managers from the group.

According to the characteristics of open network computing environment and networked software applications, trust theory systematically studies its requirements for trust management models and technologies. Based on the unified formal model of trust management, it breaks through two core technologies: trust can be established and privacy can be protected. By establishing a unified trust management model, the formal description and measurement methods of trust and privacy are formed, the dynamic construction algorithm of distributed trust chain, the collusion boycott protocol of malicious entities, the privacy protection policy and disclosure protocol, and the anonymous communication mechanism are studied. Finally, the security of the power network is analyzed based on the overall structure of the established power network demand response terminal security feedback trust model. Based on the research on trust theory (Zhang et al., 2019b; Moelker, 2021), trust is divided into identity trust and behavior trust. The security feedback trust model of power grid demand response terminal is also constructed according to this principle (Charis et al., 2021), which is divided into two main parts: identity trust relationship management module and evidence collection and trust evaluation module. The overall structure is shown in Figure 1.

These two parts are also the focus of this paper. Among them, identity trust is the basis of confidentiality and integrity services, and confidentiality and integrity services provide security for behavioral trust assessment and confidential communication. At the same time, the updating and revoking of trust relationship are all based on behavioral trust evaluation.

(1) The main services provided by the security feedback trust model of power grid demand response terminals: the main services provided by the two modules of the security feedback trust model of power grid demand response terminals: identity trust

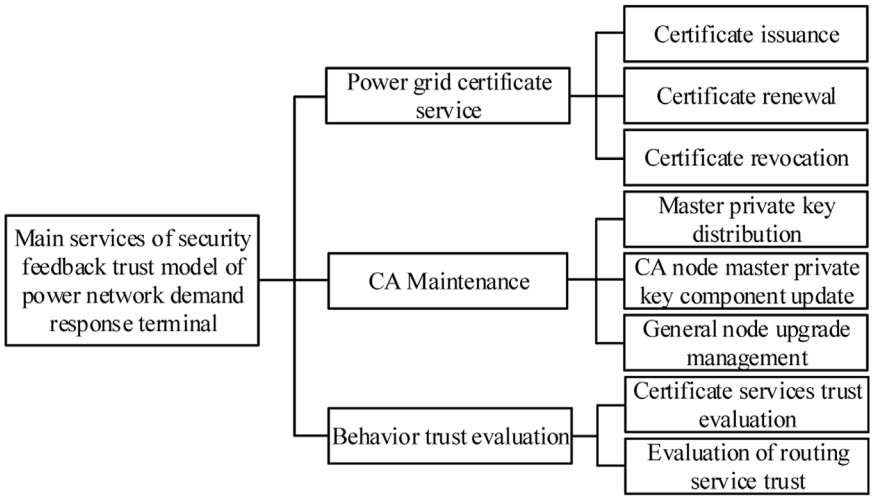

FIGURE 2
Main services of security feedback trust model of power network demand response terminal.

relationship management and evidence collection and trust evaluation include: power grid certificate service, CA maintenance and behavior trust evaluation (Tung et al., 2021). The main services of the security feedback trust model of power grid demand response terminals are shown in Figure 2.

Power gridcertificate service is responsible for establishing, updating and revoking the identity trust relationship between power grid nodes. The specific operations can be expressed as certificate issuing, updating and revoking. CA maintenance mainly includes the distribution of master and private key components in the initialization phase of the power grid (Hu et al., 2021), approving the upgrading of trusted general nodes to CA nodes, allocating master and private components to them, periodically updating the master and private key components of CA nodes, and depriving untrusted CA nodes of the authority to issue certificates. The services provided by behavior trust evaluation are mainly based on direct observation and trust recommendation of other nodes. The CA node's certificate service behavior and routing forwarding behavior of all nodes are evaluated. The trust value obtained is used as the basis for certificate revocation, master private key component update, routing, and other decisions.

(2) Storage method of power grid node trust information: In order to ensure the normal operation of power grid demand response terminal security feedback trust model, each power grid node needs to store three information bases: local information base, trust information base and certificate base.

The local information base mainly stores the node's own identity ID_{c_i}, public/private key pair PK_i/SK_i and the corresponding certificate version number m_i, the demand response terminal's primary public key PSK, the local time T_i, the demand response terminal's primary private key component S_i and the corresponding primary private key component version number. The local time is used as the standard for power grid nodes to determine whether the certificates of other nodes are expired. Therefore, after node c_i certificate is updated, other nodes will not immediately obtain c_i latest certificate, and may still use c_i old public key to communicate with it. c_i only when other nodes are aware that they are still using their old public key, will they notify the other party of their latest certificate. To ensure that c_i can decrypt the information encrypted by the old public key, c_i still retains the certificate information of the previous version after the certificate is updated.

The trust information base mainly stores some data related to identity trust and behavior trust as the basis for trust evaluation and certificate decision (Liu et al., 2019; Goyat et al., 2021). In theory, the local trust information base needs to store the information of all nodes in the power network, so it does not store large bit data information. After the power grid node interacts with a new node, the identity ID of the new node will be added to the local trust information base, and the corresponding information will be refreshed continuously according to the status and behavior of the new node.

The certificate store mainly stores the public key, session key and other information of other power network nodes that communicate with the local node. The certificate store mechanism reduces the number of certificate exchanges and communication between nodes. Because the storage space of nodes is limited, the certificate library does not store the information of all nodes in the power grid, but refreshes the certificate library according to the policy cycle.

(3) The main work of the security feedback trust model (Zhang et al., 2021b) of power network demand response terminal can be summarized as: providing three services: power network certificate management, CA maintenance and behavior trust evaluation.

The whole life cycle of power network can be divided into two stages (Huang et al., 2022): initialization and normal operation. In order to establish a secure communication environment in the power network, the first step is to realize the identity trust between communication nodes, that is, to conduct identity authentication. The process of authentication is also the process of establishing the initial trust relationship between nodes. In the initialization phase of

the power network, the trusted management center randomly generates the master public/private key pair of the demand response terminal, decomposes the master private key, distributes it to all CA nodes in the power network, and then publishes the master public key and master private key verification parameters of the demand response terminal to exit the power network. Each power grid node needs to apply to a trusted management center offline to obtain a signature certificate binding identity and public key before it can successfully enter the power grid. After the initialization phase of the power network is completed, the power network can enter the normal operation phase.

In the normal operation stage of power network, the main work of the security feedback trust model of power network demand response terminal is as follows: CA nodes cooperate to periodically update public key certificates for each node; Revoke the certificate of the illegal node, that is, remove the trust relationship with the illegal node; CA nodes cooperate to approve the trusted general node to be upgraded to CA node, and calculate and allocate the master private key component of the demand response terminal for the node that approved the upgrade; Periodically update the master and private key components of the demand response terminal mastered by each CA node; Evaluate the behavior trust of other nodes.

Power grid nodes establish identity trust relationship with other nodes by using signature certificates bound by identity and public key. Public key encryption is computationally complex and expensive. Therefore, after the nodes of the power network mutually authenticate their identities by exchanging public key certificates, they negotiate a session key each session, and use symmetric cryptographic algorithm for secure communication. In this way, the confidentiality of communication between power grid nodes is realized, which fundamentally prevents malicious acts such as eavesdropping, impersonation and tampering from hackers, and also provides basic security guarantees for trust evaluation.

During the validity period, the certificate of a power grid node may become invalid for various reasons, such as the node is damaged or the private key of the node is obtained by hackers. Therefore, certificate revocation mechanism must be provided for certificate service of power grid. The trust based command and control mechanism is used to revoke the node certificate of power network. After the power grid node discovers the malicious behavior of node c_i, it broadcasts an accusation against c_i certificate to the power grid. After node c_i receives an accusation about c_i, it first judges whether the node issuing the accusation is credible. If so, it accepts the accusation. When c_j receives a valid accusation about c_i that reaches the threshold value, c_j marks c_i certificate as invalid in the local trust repository, that is, revokes c_i certificate locally.

The main work of CA maintenance of power network demand response terminal security feedback trust model is to approve trusted general power network nodes to be upgraded to nodes, and regularly update the master and private key components of CA nodes. This is also the two main mechanisms to realize the dynamic change of CA node set based on trust. A general power network node can apply to CA node for upgrading after it has survived in the power network for a period of time. Each CA node determines whether to generate a master private key sub component for it according to the trust value of this node. The threshold number of master private key sub components can be combined to generate a new master private key component.

The above certificate service and CA maintenance of power grid are guaranteed by behavior trust evaluation mechanism. At the same time, the behavior trust evaluation mechanism can also solve the routing security problems from within the power network. The method of probability theory is used to realize behavior trust evaluation mechanism. Power network nodes can evaluate the credibility of CA node's certificate service behavior and all node's routing and forwarding behavior. The nodes of power network dynamically select routing and certificate services based on behavior trust value.

3.2 Establishing, updating and revoking identity trust relationships

The establishment of identity trust relationship and the confidential transmission of information in the security feedback trust model of power network demand response terminals enhance the security and credibility of the trust evaluation process (Hongal and Shettar, 2020; Zhang et al., 2021c). Behavioral trust evaluation can not only achieve secure routing and improve power network performance, but also further improve the security and reliability of the verification process.

The security feedback trust model of power network demand response terminal is mainly divided into two stages in the entire life cycle of the power network: the initialization stage of the power network and the normal operation stage of the power network, as shown in Figure 3.

The demand response terminal of the whole power network has a master public/private key pair (PSK, SSK), which is generated by the offline trusted management center and provides the binding service of power network node identity ID and public key signature. The master private key SSK is shared by CA nodes in the (z, x) threshold mode. Any node smaller than z cannot recover any information of the master private key. Each node generates a user public/private key pair PK_i/SK_i, which is used for authentication and secure exchange of session keys between power grid nodes. The power grid node c_i can successfully join the power grid only after obtaining the signature certificate bound by ID and PK_i offline, and the certificate update is completed by the CA node in the power grid. The node adds a serial number to the communication message to prevent hacker attacks in the power network.

3.2.1 Establishment of identity trust relationship

The power grid node generates public/private key pair (PK_i, SK_i) by itself, obtains the binding certificate of identity and public key through the offline management center, and joins the power grid with the legal certificate. The trusted management center G assigns a globally unique ID to the new node c_i of the power network, issues a certificate with the master private keys SSK and c_i of the demand response terminal, and finally transmits the latest set of power network nodes ID to c_i.

Power grid nodes can enter the power grid by carrying the binding certificate of identity ID and public key issued by the master private key of the demand response terminal. They can obtain each other's public key and establish the identity trust relationship by exchanging signature certificates with other nodes. At the same time, the power network node identity ID is distributed by the trusted management center and signed by the master private key of the demand response terminal, which ensures the uniqueness of ID in the power network and effectively prevents hackers from impersonating the power network node identity and denying the identity of the node.

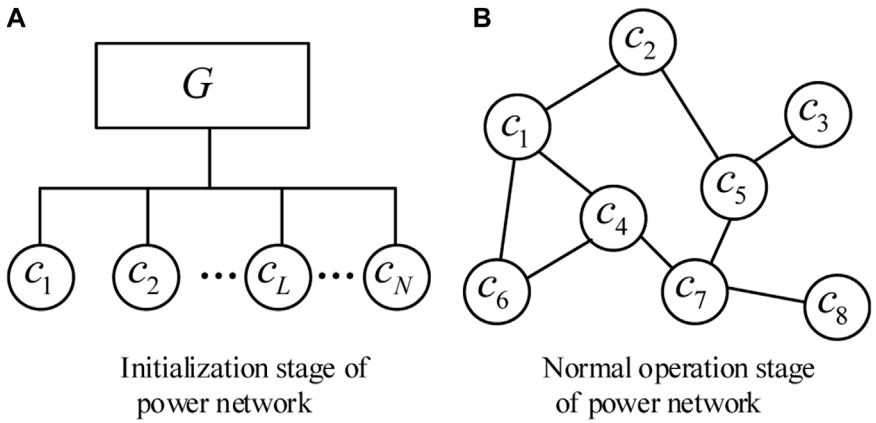

FIGURE 3
(A) Initialization stage and **(B)** normal operation stage of power network.

3.2.2 Update of identity trust relationship

It is insecure for power network nodes to use a certificate throughout the life of the power network, that is, the public/private key pair of power network nodes will not change all the time (Sui et al., 2020; Li et al., 2021c; Moorthy et al., 2021). The longer a node uses the same certificate, the greater the probability of hacker attack. Therefore, the security feedback trust model of power network demand response terminal must have the mechanism of node certificate update.

The distributed verifiable signature scheme (Han et al., 2019) is adopted to update the certificate of power grid nodes. The specific steps are as follows:

Step 1: Power grid node c_i applying for certificate update sends a certificate update request to its trusted CA node c_j. The content of the new certificate is signed with $SK_i^{(T)}$ to verify the identity of c_i, and ensure that c_i really owns the $CERT_{c_i}^{(T)}$ it claims. All contents are encrypted with $PK_j^{(T)}$, which is to authenticate the identity of CA node and prevent other hackers from damaging the contents of the new certificate.

Step 2: CA node c_j receiving the certificate application first retrieves the local trust information table. If it is determined that c_i certificate has not been revoked and c_i behavior trust value is greater than the threshold value, it will sign the certificate using its master private key component S_j, and the resulting signature certificate component is:

$$cert_{ij} = S_{S_j L_j(0)}\left(ID_{c_i}, PK_i^{(T+1)}, CM_i^{(T+1)}\right) \tag{1}$$

Then send $S_{PK_i^{(T+1)}}(cert_{ij}, H(cert_{ij}, J^{S_j}))$ to c_i. At the same time, broadcast the primary private key verification parameters J and V. The certificate components are transmitted with $PK_i^{(T+1)}$, preventing hackers from damaging the certificate components.

Step 3: After power grid node c_i receives the $(cert_{ij}, H(cert_{ij}, J^{S_j}))$ sent by CA node S_j, it needs to verify the correctness of $cert_{ij}$. c_i is calculated by using the mastered verification parameters J and V:

$$J^{S_j} = J^{SSK+a_1c_j+\cdots+a_{k-1}c_j^{k-1}} \equiv J^{SSK} \cdot (J^{a_1})^{c_j} \cdots (J^{a_{k-1}})^{c_j^{k-1}} \pmod{c} \tag{2}$$

c_i is obtained by calculating J^{S_j} from $cert_{ij}$ provided by c_j and himself, and then $validate_i = H(cert_{ij}, J^{S_j})$ is obtained. If $validate_i$ is equal to $H(cert_{ij} + J^{S_j})$ sent by S_j, $cert_{ij}$ is accepted, and the trust degree of power grid nodes is improved; Otherwise, discard $cert_{ij}$ and reduce the trust of S_j.

Step 4: Power grid node c_i combines k verified signature certificate components collected to finally obtain the certificate issued by SSK:

$$CERT_i^{(T+1)} = \prod_{j=1}^{k} cert_{ij} = \left(ID_{c_i}, PK_i^{(T+1)}, CM_i^{(T+1)}\right)^{SSK} \tag{3}$$

3.2.3 Revocation of identity trust relationship

The certificate of a power network node may become invalid during its validity period for various reasons. Therefore, the security feedback trust model of power network demand response terminals must have a certificate revocation mechanism. The security feedback trust model of power grid demand response terminal mostly adopts the distributed storage of CRL list, that is, each power grid node maintains its own CRL list. However, this method takes up a lot of storage resources of power grid nodes. Therefore, the revoked certificate is marked with the certificate revocation identifier.

If the power grid node finds the hacker attack of node c_i, it marks c_i certificate as revoked in the local trust information base, clears c_i revocation count, and broadcasts a charge against node c_i certificate to the power grid. The revocation of identity trust relationship based on trust evaluation and threshold value can effectively prevent malicious accusations of hackers attacking nodes.

3.3 Behavior trust evaluation and synthesis

In the security feedback trust model of power network demand response terminal, the establishment, update, and revocation of identity trust relationship and the security routing of power network are all based on behavior trust evaluation. The accuracy and rationality of trust evaluation will directly affect the security and efficiency of the security feedback trust model of power network demand response terminals.

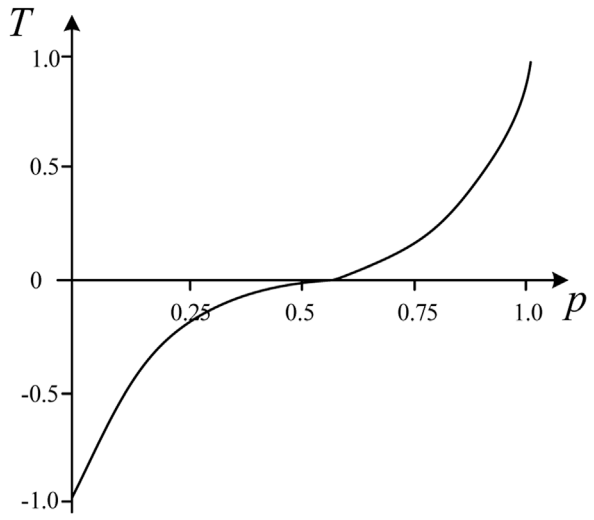

FIGURE 4
Value of $T\{c_i\colon c_j, action\}$

3.3.1 Behavior trust measurement

It can be seen from the definition of trust that it is an uncertain measurement standard. Therefore, it lacks theoretical support to directly express trust with probability value or mathematical expectation. On the basis of information theory, trust is established and measured, and the value of trust is expressed by entropy.

Trust is the relationship established between two entities (power grid nodes) to perform a specific behavior. Suppose $\{c_i\colon c_j, action\}$ represents entity c_i, trust entity c_j will perform behavior *action*, and $T\{c_i\colon c_j, action\}$ represents trust degree, that is, trust degree.$p = P\{c_i\colon c_j, action\}$ represents the probability that c_i believes c_j will perform action *action*. According to the concept of entropy in information theory, there are:

$$T\{c_i : c_j, action\} = \begin{cases} 1 - W(p), & 0.5 \le p \le 1 \\ W(p) - 1, & 0 \le p < 0.5 \end{cases} \tag{4}$$

In Formula (4), $W(p) = -p\log_2(p) - (1-p)\log_2(1-p)$. The value of $T\{c_i\colon c_j, action\}$ is shown in Figure 4.

It can be seen that the trust degree is a continuous real value between $[-1, 1]$ and increases with the increase of *a posteriori* probability p.

3.3.2 Behavior trust evaluation and synthesis

The overall trust T_T of power grid node c_i to c_j mainly comes from the direct trust D_T established through the observation of c_j behavior and the recommendation of other entities to c_j, that is, the indirect trust R_T to c_j. In essence, trust recommendation is a process of trust transmission, and trust recommendation between different power grid nodes also realizes trust transmission.

(1) Direct trust value calculated according to observation: establish a direct mutual trust relationship with neighboring nodes through observation, and the goal is to obtain the direct trust value for the node according to the previously observed behavior of neighboring nodes.

Use *a posteriori* probability to calculate the direct trust. Suppose c_i has requested c_j to execute action *action* for N_u times and c_j has executed action *action* for K_u times during the u observation, then:

$$P\{c_i : c_j, action\} = \frac{1 + \alpha^{T_c - T_m} K_m}{2 + \alpha^{T_c - T_m} N_m} \tag{5}$$

In Formula (5), $\alpha \in [0, 1]$ is a forgetting factor determined by the speed of c_j behavior change. The worse the stability of c_j, the lower the value of α. T_c represents the current time point, while T_m represents the time of each observation.

(2) Indirect trust value is calculated based on trust transfer and composition (Ding et al., 2020; Xu, 2021): when a power grid node just joins the power grid or changes its location, in order to establish trust with the target node without interactive experience with the target node, the recommendation of other nodes is mainly used to obtain the trust value of the target entity. Recommendation is essentially a process of trust transmission.

Let $R_{c_ic_c} = T\{c_i\colon c_c, recommendation\} = T_{Tc_ic_c}$ and $T_{Tc_cc_j}$ be the overall trust value of c_c to c_j. Among them, trust transfer includes:

$$R_{Tc_ic_cc_j} = R_{c_ic_c} T_{Tc_cc_j} \tag{6}$$

Trust composition is the process of synthesizing the recommended trust values from two or more channels to the target node into indirect trust values to the target node according to certain rules. On this basis, using the weight maximization algorithm (Yang et al., 2022), the trust value of the intermediate node on each recommended path is taken as the trust weight, and the trust composition is performed. Then we can use Formula (7) to calculate c_i indirect trust value of c_j obtained through c_C and c_D recommendation:

$$R_{Tc_ic_j} = \frac{R_{c_ic_C}\left(R_{c_ic_C} T_{Tc_Cc_j}\right) + R_{c_ic_D}\left(R_{c_ic_D} T_{Tc_Dc_j}\right)}{R_{c_ic_C} + R_{c_ic_D}} \tag{7}$$

When there are more than two trust recommendation paths, expand Formula (7) to comprehensively recommend the trust value from multiple trust recommendation paths as follows:

$$R_{Tc_ic_j} = \sum_{L=1}^{K} R_{Tc_ic_Lc_j} = \frac{\sum_{L=1}^{K} R_{c_ic_L}^2 T_{Tc_Lc_j}}{\sum_{L=1}^{K} R_{c_ic_L}} \tag{8}$$

In Formula (8), C_L represents the different nodes that provide c_i with the recommended value of c_j, and K represents the number of recommended paths. When c_i just joined the power grid or changed its location, it did not establish behavioral trust relationship with other nodes. In this case, to obtain the indirect trust value of the target node of the power grid, it can only request the neighbor node of the power grid to provide it. When c_i gradually establishes trust relationship with other power network nodes in the power network, it can obtain the recommended trust value of the target node through the most trusted node, and finally obtain the indirect trust of the target node.

(3) Overall trust evaluation: the overall trust $T_{Tc_ic_j}$ of power grid node c_i to c_j, the recommended trust of other nodes to c_j, and the direct trust, the indirect trust value is as follows:

TABLE 1 Parameter setting of simulation experiment.

Project	Parameter
T_m	50/s
J	0.02
V	0.01
α	0.8
β	0.5

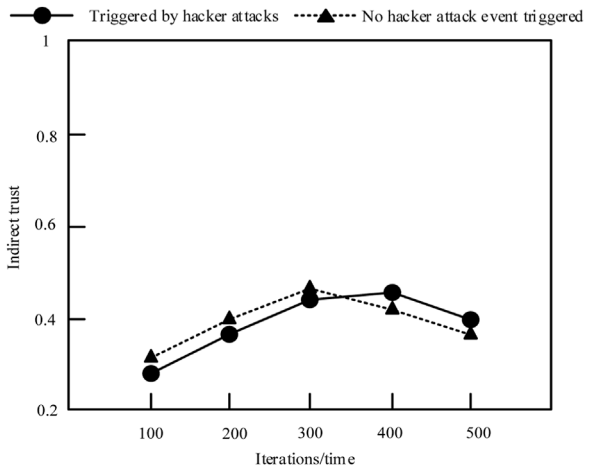

FIGURE 5
Impact of hacker attacks on power network node trust.

$$T_{T_{c_i c_j}} = \beta D_{T_{c_i c_j}} + (1-\beta) R_{T_{c_i c_j}} \tag{9}$$

In Formula (9), $\beta \in [0, 1)$ is the confidence coefficient. Confidence coefficient controls the proportion of direct trust and indirect trust in the overall trust. If c_i is newly added to the power grid or its location has just changed, and there is no direct interaction experience with c_j, then c_i trust in c_j mainly comes from the trust recommendation of other nodes to T, and Y is very small at this time. With the continuous interaction between c_i and c_j, direct trust accounts for more and more of the overall trust, and β also increases until it reaches a value less than 1.

Through the above steps, the security feedback trust model of power network demand response terminal triggered by hacker attacks is realized.

3.4 Simulation experiment and analysis

3.4.1 Setting the simulation experiment environment

In order to verify the validity of the security feedback trust model of power network demand response terminal triggered by hacker attacks, this paper uses PeerSim1.0.5 simulation software to simulate it. On this basis, it is assumed that the total number of nodes in the power network is 100 and the trust degree of each node

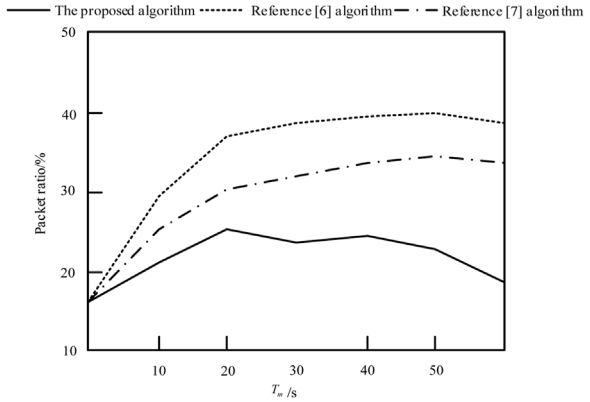

FIGURE 6
Packet ratio of malicious nodes triggered by hacker attack events in different methods.

is 0.5. Each node in the power grid has 50 files in total, and each node selectively downloads 30 times from other nodes. Each group of experiments is simulated for 10 times, and each simulation cycle is 30 times. The results of simulation experiments are average results. The simulation experiment parameter settings are shown in Table 1.

3.4.2 Analysis of the impact of hacker attacks on the trust of power grid nodes

In order to verify the validity of the security feedback trust model of power network demand response terminals, the impact of hacker attacks on the trust of power network nodes is analyzed. It is assumed that 50% of the power network has transacted with the target node, and two conditions are set under whether there is a hacker attack event triggered. The influence results on the trust level of the power network node are shown in Figure 5.

According to Figure 5, as the number of iterations increases, the impact of hacker attacks on the indirect trust of power grid nodes decreases. The reason is that the more iterations, the more similar the hacker attack ID is, and the trust given by nodes with similar IDs is roughly the same. Therefore, the security feedback trust model of power network demand response terminals can judge the hacker attacks, thereby reducing the impact of hacker attacks on the trust of power network nodes.

3.4.3 Security analysis of power network demand response terminal

On this basis, the security of the power network demand response terminal of the proposed method is verified, and the packet ratio of malicious nodes triggered by hacker attacks is taken as the evaluation index. The lower the packet ratio, the higher the security of the power network demand response terminal of the method. The calculation formula is as follows:

$$\gamma = \frac{\kappa}{\mu} \times 100\% \tag{10}$$

In Formula (10), κ is the number of malicious node packets triggered by hacker attacks, and μ is the total number of packets

TABLE 2 Comparison results of packet loss rates of different methods.

T_m/s	The proposed method/%	Reference (Zhang et al., 2019a) method/%	Reference (Alagappan et al., 2022) method/%
10	0.6	1.5	2.6
20	1.2	2.7	4.7
30	2.4	3.9	5.6
40	3.7	5.2	7.4
50	4.4	6.1	8.9

transmitted by the power network. By comparing the methods of literature (Zhang et al., 2019a), the methods of literature (Alagappan et al., 2022) and the proposed methods, we can get the packet ratio of malicious nodes triggered by hacker attacks in different methods, as shown in Figure 6.

According to Figure 6, when there is a malicious node triggered by a hacker attack event in the power grid using the methods of literature (Zhang et al., 2019a), the methods of literature (Alagappan et al., 2022) in the power grid demand response terminal, the packet rate of the malicious node triggered by the hacker attack event will increase from 16% to 40%. With the increase of the number of malicious nodes triggered by hacker attacks in the power grid, the packet ratio of malicious nodes triggered by hacker attacks will also rise rapidly. However, in the power network demand response terminal, using the proposed method, the trust of malicious nodes triggered by hacker attacks drops rapidly, and normal nodes will bypass these malicious nodes triggered by hacker attacks when routing. Therefore, the packet rate of malicious nodes triggered by hacker attacks will decrease. It can be seen that the proposed method has a high security of power network demand response terminal.

3.4.4 Mutual security analysis between power grid nodes

Further verify the interaction security between power grid nodes of the proposed method, and take packet loss rate as the evaluation index. The lower the packet loss rate, the higher the interaction security between power grid nodes of the method. The calculation formula is as follows:

$$\tau = \frac{\lambda}{\mu} \times 100\% \tag{11}$$

In Formula (11), λ is the total number of packets dropped by power grid nodes. The methods of literature (Zhang et al., 2019a), the methods of literature (Alagappan et al., 2022) and the proposed methods are compared, and the comparison results of packet loss rates of different methods are shown in Table 2.

According to Table 2, the packet loss rate of different methods increases with the increase of observation time. When the observation time reaches 50 s, the packet loss rate of the methods of literature (Zhang et al., 2019a) is 6.1%, and that of the methods of literature (Alagappan et al., 2022) is 8.9%. The packet loss rate of the proposed method is only 4.4%. It can be seen that the packet loss rate of the proposed method is low, indicating that the interaction security between nodes of the power network of the proposed method is high.

4 Discussion

In the experimental test, the proposed method can judge the hacker attacks, reduce the impact of hacker attacks on the trust of power grid nodes, and improve the interaction security between power grid nodes. Reference (Zhang et al., 2019a) method and Reference (Alagappan et al., 2022) method are based on the master-slave chain architecture of the blockchain and the zero trust network architecture to enhance the security of virtual power plants, respectively, to reduce security risks. No identity trust relationship has been established, resulting in low security between power grid nodes. But the proposed method uses convolutional neural network method in artificial intelligence technology to effectively improve the flexibility of smart grid and effectively enhance the overall anti-interference capability of power grid.

5 Conclusion

This paper proposes a security feedback trust model of power network demand response terminals triggered by hacker attacks. By analyzing the role of smart grid in power grid, the flexibility of smart grid is enhanced based on convolutional neural network in artificial intelligence technology. Aiming at the security problem of demand response terminal of power network being attacked by hackers, a security feedback trust model of demand response terminal of power network is designed based on trust theory. The distributed verifiable signature scheme is adopted to update the certificate of power network nodes. Based on information theory, trust is established and measured. The behavior trust evaluation and composition mechanism is introduced into the security feedback trust model of power network demand response terminals to achieve the credibility of power network node identity and behavior. The following conclusions are drawn:

(1) As the number of iterations increases, the impact of hacker attacks on the indirect trust of power grid nodes decreases, which indicates that the proposed method can judge the hacker attacks, thereby reducing the impact of hacker attacks on the trust of power grid nodes.
(2) The proposed method can improve the security of power network demand response terminals because of the low packet rate of malicious nodes triggered by hacker attacks.
(3) The low packet loss rate of the proposed method indicates that the interaction security between nodes of the power network is high.

The subsequent research will deeply study the storage mode and hash mapping mode of trust information on the device access network

to improve the search efficiency of resources and reduce the cost of proxy servers.

Data availability statement

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

Author contributions

Each author made significant individual contributions to this manuscript. JC: methodology, data analysis, and writing; LZ: data analysis, writing-reviewing, and editing; QS: article review and intellectual concept of the article; CZ: research and investigation, consult materials and references.

Conflict of interest

JF was employed by State Grid Shandong Electric Power Company. LZ was employed by Information and Communications Company, State Grid Shandong Electric Power Company. QS was employed by State Grid Weihai Wendeng Power Supply Company. CZ was employed by State Grid Juxian Power Supply Company.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Alagappan, A., Venkatachary, S. K., and Andrews, L. J. B. (2022). Augmenting Zero Trust Network Architecture to enhance security in virtual power plants. *Energy Rep.* 8, 1309–1320. doi:10.1016/j.egyr.2021.11.272

Charis, G., Danha, G., Muzenda, E., and Nhubu, T., (2021). Modeling a sustainable, self-energized Pine Dust Pyrolysis system with staged condensation for optimal recovery of bio-Oil. *Front. Energy Res.* 8, 594073. [J].

Cherukuri, S., Chenniboyena, R., Yarlagadda, D., Kolluru, V. R., and Razia, S., (2022). *Development of Raspberry pibot surveillance security system, confidential computing*. Singapore: Springer, 79–86.

Das, T., and Mukherjee, S. (2022). *Data privacy in IoT network using blockchain technology, intelligent systems for social good*. Singapore: Springer, 117–137.

Ding, Y., Zhao, Y., and Zhang, R. (2020). "A secure routing algorithm based on trust value for micro-nano satellite network," in Proceedings of the 2020 2nd International Conference on Information Technology and Computer Application (ITCA), Guangzhou, China, December 2020 229–235. [C]//.

Goyat, R., Kumar, G., Alazab, M., Saha, R., Thomas, R., and Kumar, R. M. (2021). A secure localization scheme based on trust assessment for WSNs using blockchain technology. *Future Gener. Comput. Syst.* 125, 221–231.

Group, R. (2022). Hacker attack on deutsche windtechnik. *Renew. Energy Monit.* 21, 10–11.

Gunjan, V. K., Kumar, A., and Rao, A. A. (2014). "Present & future paradigms of cyber crime & security majors-growth & rising trends," in Proceedings of the 2014 4th International Conference on Artificial Intelligence with Applications in Engineering and Technology, Kota Kinabalu, Malaysia, December 2014 89–94.

Han, S., Xie, M., Yang, B., Lu, R., Bao, H., Lin, J., et al. (2019). A certificateless verifiable strong designated verifier signature scheme. *IEEE Access* 7, 126391–126408. doi:10.1109/access.2019.2938898

Hongal, R. S., and Shettar, R. B. (2020). A power-efficient and quantum-resistant N-bit cryptography algorithm. *Int. J. Nat. Comput. Res. (IJNCR)* 9 (4), 18–33. doi:10.4018/ijncr.2020100102

Hu, W., Yang, Z., Chen, C., Wu, Y., and Xie, Q. (2021). A weibull-based recurrent regression model for repairable systems considering double effects of operation and maintenance: A case study of machine tools. *Reliab. Eng. Syst. Saf.* 213, 107669. doi:10.1016/j.ress.2021.107669

Huang, Z. F., Soh, K. Y., Islam, M. R., and Chua, K. (2022). Digital twin driven life-cycle operation optimization for combined cooling heating and power-cold energy recovery (CCHP-CER) system. *Appl. Energy* 324, 119774. doi:10.1016/j.apenergy.2022.119774

Jiang, W., Wang, Y., Jiang, Y., Chen, J., Xu, Y., and Tan, L. (2019). Research on mobile internet mobile agent system dynamic trust model for cloud computing. *China Commun.* 16 (7), 174–194. doi:10.23919/jcc.2019.07.014

Karthik, R., Baji, V. M. M., Kumar, M. P., Anjum, S. A., Suresh, M., et al. (2022). *Image security based on rotational visual cryptography, confidential computing*. Singapore: Springer, 87–96.

Karthik, R., Shukla, P., Lavanya, S., Naga Satish, L. L., and Sai, R. K. J. (2022). *Deep transfer learning for detecting cyber attacks, confidential computing*. Singapore: Springer, 113–124.

Li, C., Qu, Q., Gao, W., Xiao, X., Yuan, P., and Wang, X. (2021). "Heterogeneous network selection strategy based on power wireless communication system," in Proceedings of the 2021 5th International Conference on High Performance Compilation, Computing and Communications, Guangzhou China, June 2021 1–6.

Li, J., Liu, H., Wang, D., and Bi, T., (2021). Classification of power quality disturbance based on S-transform and convolution neural network. *Front. Energy Res.* 9, 325.

Li, S., Lu, D., Wu, X., Han, W., and Zhao, D. (2021). Enhancing the power grid robustness against cascading failures under node-based attacks. *Mod. Phys. Lett. B* 35 (09), 2150152. doi:10.1142/s0217984921501529

Liu, G., Yang, Q., Wang, H., and Liu, A. X. (2019). Trust assessment in online social networks. *IEEE Trans. Dependable Secure Comput.* 18 (2), 994–1007. doi:10.1109/tdsc.2019.2916366

Liu, Z., Fan, Y., Wang, Y., Miao, Z., Sun, Y., and Miao, X. (2020). Evaluation trust model of block chain information capacity based on subjective logic. *J. Hebei Univ. Nat. Sci. Ed.* 40 (2), 431–437.

Moelker, R. (2021). *SHAPE we trust! Trust theory put to the test within an ambidexterious headquarters. The yin-yang military*. Cham, Switzerland: Springer, 213–224.

Moorthy, R. S. K., Liu, G., Chinthavali, M., Choi, J., and Starke, M., (2021). Architecture of a residential solid state power substation (SSPS) node Proceedings of the 2021 IEEE power & energy society innovative smart grid technologies conference (ISGT). Washington, DC, USA, February 2021 , 1–5.

Prasad, P. S., Beena Bethel, G. N., Singh, N., Kumar Gunjan, V., Basir, S., and Miah, S. (2022). Blockchain-based privacy access control mechanism and collaborative analysis for medical images. *Secur. Commun. Netw.* 2022, 9579611–9579617. doi:10.1155/2022/9579611

Ren, H., Hou, Z. J., Vyakaranam, B., Wang, H., and Etingov, P. (2020). Power system event classification and localization using a convolutional neural network[J]. *Front. Energy Res.* 8, 607826.

She, J., Shi, T., Xue, S., Zhu, Y., and Cao, H., (2021). Diagnosis and prediction for loss of coolant accidents in nuclear power plants using deep learning methods. *Front. Energy Res.* 10, 186.

Sui, B., Chen, X., Li, Z., Zhao, J., and Tian, J. (2020). Research on multi-node frame early warning system of power grid based on abnormal data extraction[C]//Journal of physics: Conference series. *IOP Publ.* 1654 (1), 012020. doi:10.1088/1742-6596/1654/1/012020

Sun, M., Wang, Q., He, J., Huang, H., Huang, Y., Shen, X., et al. (2022).Research on automatic scanning method of network vulnerabilities in power system *J. Phys. Conf. Ser.*, 2290. 112036. doi:10.1088/1742-6596/2290/1/012036

Tung, N. T., Nam, P. M., and Tin, P. T. (2021). Performance evaluation of a two-way relay network with energy harvesting and hardware noises. *Digital Commun. Netw.* 7 (1), 45–54. doi:10.1016/j.dcan.2020.04.003

Wang, W., Wang, C., Guo, Y., Yuan, M., and Gao, Y. (2021). Industrial control malicious traffic anomaly detection system based on deep autoencoder. *Front. Energy Res.* 8, 555145. [J].

Xu, Q. (2021). Wireless sensor networks secure routing algorithm based on trust value computation. *Int. J. Internet Protoc. Technol.* 14 (1), 10–15. doi:10.1504/ijipt.2021.10036582

Xu, X., and Hong, L. (2022). Instantaneous and limiting behavior of an n-node blockchain under cyber attacks from a single hacker. *arXiv Prepr. arXiv* 13 (2), 352–359.

Yang, C., Ma, B., Yin, B., and Chen, Y. (2022). Model predictive control for compound power supply based on fuzzy weight. *Comput. Simul.* 39 (04), 103–109.

Zhang, M., Zhao, W., Shi, W., and Zhou, H. (2021). Privacy protection method of electric power network based on blockchain[C]//Journal of physics: Conference series. *IOP Publ.* 1744 (2), 022009. doi:10.1088/1742-6596/1744/2/022009

Zhang, N., Dai, H., Wang, Y., Zhang, Y., Yang, Y., Lund, P., et al. (2021). Power system transition in China under the coordinated development of power sources, network, demand response, and energy storage. *Wiley Interdiscip. Rev. Energy Environ.* 10 (2), e392. [J].

Zhang, N., Dai, H., Wang, Y., Zhang, Y., and Yang, Y. (2021). Power system transition in China under the coordinated development of power sources, network, demand response, and energy storage. *Wiley Interdiscip. Rev. Energy Environ.* 10 (2), 392–399. doi:10.1002/wene.392

Zhang, X., Gong, Y., and Spece, M. (2019). Trust decision model for online consumer evaluation: Deeper uncertainty integration in evidence theory approach. *J. Intelligent Fuzzy Syst.* 36 (5), 4257–4264. doi:10.3233/jifs-169983

Zhang, Z., Zhong, C., Guo, S., and Wang, F. (2019). "A master-slave chain architecture model for cross-domain trusted and authentication of power services," in Proceedings of the 2019 7th International Conference on Information Technology: IoT and Smart City, Shanghai China, December 2019 483–487.