Research on Quantitative Security Protection Technology of Distribution Automation Nodes based on Attack Tree

Yinfeng Han*, Yong Tang, Xiaoping Kang, Hao Jiang, Xiaoyang Song
Ningbo Power Supply Company, State Grid Zhejiang Electric Power Company, Zhejiang, China

***Abstract*—In order to improve the security of distribution automation system nodes and ensure the safe operation of distribution network, a quantitative security protection technology for distribution automation nodes based on attack tree is proposed. This paper analyzes the factors of node risk assessment of the distribution automation system, and through the evaluation and analysis of node vulnerabilities; it discovers the faulty nodes in the distribution automation system in advance. Based on the node vulnerability evaluation results of the distribution automation system, the risk of the distribution automation system is comprehensively evaluated using the attack tree. Establish the distribution network control model under network attack, locate the fault node, and use trusted computing technology to design trusted distribution terminals. When the amount of data is large, more effective symmetric encryption algorithm SM4 is required to achieve node security protection in the distribution network automation system. The experimental results show that the method has high fault node location accuracy, low reliability calculation time, and the distribution automation system network has certain robustness, which fully verifies the application effect of the method.**

Keywords*—Attack tree; security protection; risk assessment; fault node location; trusted computing; SM4 encryption algorithm

I. INTRODUCTION

A distribution grid failure is an unpredictable situation that can cause the entire system to operate unbalanced. For various reasons, faulty nodes may appear between regions of the distribution network [1,2]. Illegal access to the power grid to steal power is very likely to cause the access point to become a faulty node, which will lead to unpredictable technical problems in the power system. In addition, due to this part of illegal access to unaccounted electricity consumption, from an economic point of view, this problem will seriously affect the income of the power company. Therefore, the research on quantitative security protection of distribution network automation system nodes is urgent [3,4].

Literature [5] proposes a network security protection method of distribution network automation system based on independent security chip, designs a dual protection scheme based on "network layer + application layer", and proposes a one-time password authentication protocol based on the combination of SM2, SM3 and SM4 national secret algorithms and message authentication codes, so as to realize bidirectional identity authentication and business data encryption between distribution master station and distribution terminal. Ensure the integrity and confidentiality of communication data, and solve the network security protection problem of distribution network automation system. Literature [6] proposes an active distribution network security protection method based on trusted computing. Firstly, the information security problems existing in the power generation, transmission, distribution and utilization of the active distribution network are analyzed. Then, referring to the design of power distribution automation system, the overall security and reliability protection scheme is proposed for the regional energy Internet. According to the scheme, a trusted chain is established to ensure the reliability of nodes, network connections and applications. Finally, an example is given to verify the scheme. SM2 and SM4 encryption algorithms are mainly used for data transmission and storage. Considering that the downlink data will have a large number of repeated cryptographic operations. Batch certification method is adopted. By using Merkle hash tree to merge multiple authentication requests, the data processing efficiency is improved. In addition, some scholars have proposed the key technologies of information security protection of active distribution network. Firstly, the characteristic model of active distribution network architecture is analyzed, and the trusted protection environment model of active distribution network is described in combination with the existing typical application mode of active distribution network security protection; Secondly, the embedded trusted distribution terminal is designed for the application scenario of the embedded distribution terminal, and the active distribution network networking model based on the IEC61850 standard is designed for the information flow interaction and data analysis between the various levels of the active distribution network; Thirdly, in view of the complementary coupling and flat management structure requirements of the active distribution network, combined with the supporting role of the active distribution network for the regional energy Internet, the prefecture-level regional energy based on multi-level energy-information routers and energy-information switches is defined. Based on the Internet system model, a trusted in-depth protection system for prefecture-level regional energy Internet security based on Trusted 2.0 technology has been constructed. Finally, combined with the advanced nature of Trusted 3.0 technology, starting from energy nodes, with trusted computing as the basic idea, autonomous controllability as the goal, and safety immunity as the characteristic, the trusted protection scheme is further optimized and adjusted, its safety protection has certain engineering application and reference value.

*Corresponding Author.

In order to improve the security of distribution automation system nodes and ensure the safe operation of distribution network, a quantitative security protection technology for distribution automation nodes based on attack tree is proposed. This paper analyzes the factors of node risk assessment of the distribution automation system, and through the evaluation and analysis of node vulnerabilities; it discovers the faulty nodes in the distribution automation system in advance. Based on the node vulnerability evaluation results of the distribution automation system, the risk of the distribution automation system is comprehensively evaluated using the attack tree. Establish the distribution network control model under network attack, locate the fault node, and use trusted computing technology to design trusted distribution terminals. When the amount of data is large, more effective symmetric encryption algorithm SM4 is required to achieve node security protection in the distribution network automation system. Finally, the experiment proves the effectiveness of the design method.

II. Quantitative Assessment of Node Risk Distribution Network Automation System

A. Risk Assessment Factors of Distribution Network Automation System Nodes

It is very important to take an effective quantitative risk assessment method to objectively and accurately assess the risk degree of the power distribution system to ensure the safe, stable and reliable operation of the power distribution system. Here, for the node risk of the distribution network automation system, the node voltage over-limit risk and the line power flow over-limit risk are mainly considered. Each risk is represented by the probability of occurrence, and the risk of the distribution system is measured by establishing a comprehensive system over-limit risk index.

1) The probability calculation of the node voltage exceeding the limit is shown in formula (1):

$$U_i = Q_r\left(U_i > U_{i\max}\right) = 1 - \left[K\left(U_i\right) - K\left(U_{i\min}\right)\right] \quad (1)$$

In the formula: U_i is the voltage amplitude of node i; $U_{i\max}$ and $U_{i\min}$ are the upper and lower limits of the node voltage; $K\left(U_i\right)$ is the probability distribution function of the voltage amplitude of node i.

2) The probability calculation of line power flow exceeding the limit is shown in formula (2):

$$Q_r\left(F_j\right) = 1 - Y\left(G_j\right) \quad (2)$$

In the formula: F_j is the conveying capacity of branch j, MVA; G_j is the rated conveying capacity of branch j, MVA; $Y\left(G_j\right)$ is the probability distribution function of the conveying capacity of branch j.

3) The output change of the distributed power generation in the distribution network may cause the node voltage and line power flow to have the risk of exceeding the limit. In order to evaluate the various kinds of over-limit risk R_f separately, a comprehensive over-limit risk index is defined here, such as formula (3) as shown:

$$R_f = \frac{1}{M}\sum_{i=1}^{M}\left(P_g - P_f\right) \quad (3)$$

In the formula: M is the number of system nodes or lines; P_g and P_f are the over-limit probabilities of node voltage or branch power flow before and after access to distributed power. This index can be used to measure the comprehensive risk of exceeding the limit of voltage and power flow of the distribution system, which is referred to here as the comprehensive risk of exceeding the limit of node voltage and the comprehensive risk of exceeding the limit of line power flow.

B. Node Vulnerability Assessment of Distribution Network Automation System

When the nodes in the distribution network automation system are disturbed or influenced by the outside world, it is easy to cause successive failures of the components in the system, resulting in large-scale power outages. Through node vulnerability assessment and analysis, the faulty nodes in the distribution network automation system are found in advance, and the improvement of these faulty nodes will reduce the possibility of accidents in the distribution network automation system.

The power distribution network can be simplified as an undirected weighted sparse graph with M nodes and L edges by the complex network definition. The traditional complex network theory has its statistical characteristics, such as characteristic path length, degree, clustering coefficient and betweenness, and can be directly used as an index for risk assessment of distribution network automation system nodes. This paper considers that the structure of distribution network and transmission network is different, so these statistical characteristics need to be improved to meet the structural characteristics of distribution network.

The traditional node degree is defined as the number of nodes connected to the node, and the average degree of the network can be obtained by averaging the degrees of all nodes. The node degree can reflect the importance of the nodes in the network, that is, the node with a larger degree is more important in the network, and the more vulnerable it is. When the distributed power source is connected, the number of system nodes is not changed. Therefore, the node degree of the node connected to the distributed power source should be increased by 1. The calculation formula is:

$$s_i = s_{idp} + 1 \quad (4)$$

In the formula: s_i is the degree of access to the distributed power node; s_{idp} is the degree of the original node of the access to the distributed power node.

Since the distribution network is mostly radial network, which is relatively sparse compared with the transmission network, it is difficult to compare the differences between nodes with the same degree only considering its own node degree. The idea of cohesion is introduced here, and the node degree is calculated considering the influence of the nodes connected with node i:

$$Ms_i = \frac{s_i}{\overline{s_i}} \times \int_i^M D_{iM} \tag{5}$$

In the formula: $\overline{s_i}$ is the average degree of nodes; D_{iM} is the set of all nodes connected to node i.

It is difficult to judge the vulnerability of a node scientifically and comprehensively only by a single node vulnerability index. The node vulnerability index proposed based on the complex network theory mainly analyzes the vulnerability of the node from the structure. The voltage over-limit risk index analyzes the node's vulnerability from the aspect of fault risk. Combining the two, it is proposed that the node's comprehensive vulnerability index can make up for the shortcomings of the two and make a comprehensive judgment.

In this paper, the structural vulnerability index obtained based on the complex network theory is given weight by using the analytic hierarchy process [7,8] (AHP). Through consulting experts, it is equally important to set the node degree and the node intermediate number, and the node active power injection power is more important. The comparison matrix can be obtained by applying the analytic hierarchy process:

$$S = \begin{bmatrix} 1 & 1 & 1/3 \\ 3 & 3 & 1 \\ 1 & 1 & 1/3 \end{bmatrix} \tag{6}$$

The matrix satisfies the requirement of consistency, and the weights of node degree, node betweenness and active power injection power are obtained as 0.2, 0.2 and 0.6, respectively. The structural vulnerability index MS_i of the distribution network node i based on the complex network theory obtained by the AHP is:

$$Mw_i = 0.2 \times Ms_i + 0.2 \times Mq_i + 0.6 \times Mr_i \tag{7}$$

Due to the differences in the units and orders of magnitude of the above indicators, they cannot be directly added. The unit and order of magnitude of the indicators should be normalized first. In this paper, the maximum value of each indicator is taken as the benchmark for normalization, and the data is normalized to [0,1] interval.

Combined with the risk theory, the structural vulnerability index of node i is multiplied by the risk value of the node as the comprehensive vulnerability index of node i, and its expression is:

$$M_i = Ms_i \times M_{w_i} \tag{8}$$

C. Comprehensive Risk Assessment of Distribution Network Automation System

Based on the node vulnerability assessment results of distribution network automation system, the attack tree is further used to comprehensively evaluate the risk of distribution network automation system.

1) Definition of attack tree: The attack tree model [9,10] is a method of modeling security threats to the system, which represents each attack against the system in the form of a tree structure. The root node of the tree represents a goal to be achieved by a network attack, and the leaf nodes represent possible means to achieve this attack purpose. Each path from the root node to the leaf node represents a complete attack process to achieve this attack goal. The nodes of the attack tree are divided into two types: AND (AND) nodes or AND (OR) nodes. Among them, and node means: only after all child nodes are implemented, this node can be implemented, and the task will continue to be passed up; or node means: as long as one of the child nodes has been implemented, this node can be implemented, and the task will be up first-level delivery.

2) Stage division of intrusion process: Every complete invasion process will be very complex, and any two kinds of invasion are also very different. Therefore, it is very difficult and unrealistic to model the whole intrusion process. Similarly, it is unrealistic to use a single attack tree to model all intrusions and attacks against the distribution network automation system. The constructed attack tree will be very large, which is not conducive to analysis and maintenance.

Based on the above reasons, this paper considers dividing the intrusion process into several stages, and each stage has a stage target, and models these stages respectively. By modeling in stages, the complexity of constructing the attack tree can be greatly reduced. Specifically, a complete intrusion process can be divided into the following seven stages:

a) Host survey: search for a distribution network automation system node as an attacked target.

b) Vulnerability discovery: Discover the security loopholes on the target distribution network automation system nodes.

c) Target penetration: use the security loopholes of the distribution network automation system nodes to obtain unauthorized access rights.

d) Privilege escalation: Obtain privileged privileges on the nodes of the distribution network automation system.

e) Hidden and hidden: cover up the activity track, in order to prepare for the next invasion of the distribution network automation system node.

f) Grab information: obtain and modify the data and information on the nodes of the distribution network automation system.

g) Springboard attack: Use the controlled node as a springboard to launch attacks on other nodes.

In the following, according to the stages of the attack process, each stage is regarded as the root node of an attack tree, and an attack tree is constructed for each stage of the network attack.

3) Comprehensive risk assessment: Comprehensive risk assessment is an important process of risk management, and the risk is often expressed by the product of the loss caused by the event and the probability of the event, namely:

$$R_h = L_h \times P_h \tag{9}$$

In the formula: L_h is the loss caused by the event; P_h is the probability of the event occurring.

The root node in the attack tree represents the ultimate goal of the attacker, so the ultimate goal of the risk assessment based on the attack tree is to determine the risk value of the root node of the attack tree, the attack path that affects this value, and the attack method most likely to be exploited by the attacker, so that technicians can formulate corresponding defense countermeasures according to the risk assessment results. The specific steps of the comprehensive risk assessment method for distribution network automation system based on attack tree proposed in this paper are as follows:

a) Determine the attack target and establish the attack tree model of the system.

b) Select the appropriate evaluation index, and quantify the index of the attack tree leaf node.

c) Calculate the probability P_h of leaf node (attack event) occurrence.

d) Calculate the probability P_s of attacking the root node of the tree (that is, the attacker successfully achieves the final attack target).

e) Analyze the loss L_t caused by the realization of the attack target of attacking the root node of the tree, and use formula (9) to calculate the risk value of the root node.

f) Analyze the attack sequence and calculate the probability P_{hi} of each attack sequence.

g) Judging and analyzing the attack paths and methods most likely to be exploited by attackers according to the results of comprehensive risk assessment.

III. Quantitative Security Protection of Distribution Automation Nodes

A. Construction of Distribution Network Control Model under Network Attack

There are two types of network attacks for multi-node systems: centralized attacks and decentralized attacks. A decentralized attack is to launch an attack on all nodes in the area, which has a wide range of influence, but requires a higher degree of control of the attacker. Concentrated attack is to launch an attack on the nodes in the area in a targeted manner. This method has a small direct impact. However, if the attack is launched against the weak nodes in the area, the target can be destroyed at a lower attack cost. Therefore, this paper mainly considers the impact of centralized attacks.

The ultimate purpose of physical attack is to destroy the power infrastructure. It is a direct effect on physical equipment. With the subjective will of the attacker, it can directly cause the abnormal operation of a large number of physical equipment, and even cause a cascading failure to cause the collapse of the power system, with great destructive power, but the concealment is weak and the attack cost is high. The network attack takes the information space as the entrance, exploits the vulnerability of the distribution network and its nodes to destroy the distribution network automation system, and finally achieves the purpose of causing large-scale power outages. Compared with physical attacks, network attacks are not easy to be detected, have a long incubation period, and have low attack costs, but they can achieve significant damage.

To sum up, network attacks can covertly realize the attacker's intention and destroy the normal operation of the distribution network automation system. In order to study the scenario where the distribution network is attacked by the network, a distribution network control model is established on the basis of the comprehensive risk assessment of the distribution network automation system. The evaluation index of the distribution network includes power supply quality, economy, safety, etc., which is called the controlled quantity in this paper, denoted by G. In general, these controlled quantities are determined by the protection action, dispatch control and user behavior of the power company, which can be described as:

$$G = R(e, v, z) \tag{10}$$

In the formula: e is protection action; v is scheduling control; z is user behavior.

Formula (10) is a nonlinear equation, and the solution of the equation is related to the input (e, v, z) and the initial state of the distribution network. In the traditional distribution network, user behavior is reflected in daily life and production activities, and is a random variable that conforms to certain laws. At this time, the distribution network is mainly controlled by dispatching and protection. The dispatching system and protection device control the distribution network according to the state detection quantity to ensure that the controlled quantity G meets the requirements of the stable operation of the distribution network.

Unlike normal scheduling, protection, and user usage behavior, attack behavior is unpredictable. Therefore, malicious control behavior is introduced into the distribution network control model, which can be expressed as:

$$G = R(e, v, z, U) \tag{11}$$

In the formula: U is the aggressive behavior.

Also, the total formula (11) is a nonlinear equation. U is sent by an attacker, and the attack may cause the controlled quantity G to deviate from the safe and stable operation requirements of the distribution network, causing a safety and stability accident. Fig. 1 is a schematic diagram of the distribution network control model under network attack.

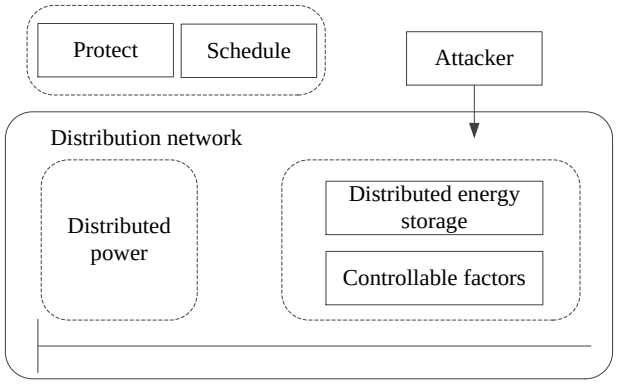

Fig. 1. Schematic diagram of distribution network control model under network attack.

B. Fault Node Location

Based on the simulation analysis of the distribution network control model under network attack, the voltage array of the distribution network nodes is obtained. According to the operation characteristics of the distribution network automation system in each iteration; the presence of fault nodes is detected. The difference between the measured voltage array and the estimated voltage array is:

$$\Delta V = V_\alpha - V_\beta \tag{12}$$

In the formula: V_α is the measured voltage array; V_β is the estimated voltage array. ΔV is zero in the absence of faulty nodes.

The area where the faulty node exists is displayed through the abnormality matrix elements, and the peak value of the elements in the faulty node area A_d shows the faulty node closest to the fault location in the distribution network automation system. The faulty node is defined as follows:

$$\forall x \in A_d : x_i \geq x_k \tag{13}$$

This method can detect the existence of the faulty node and determine the location of the faulty node. The flow chart of the positioning method is shown in Fig. 2.

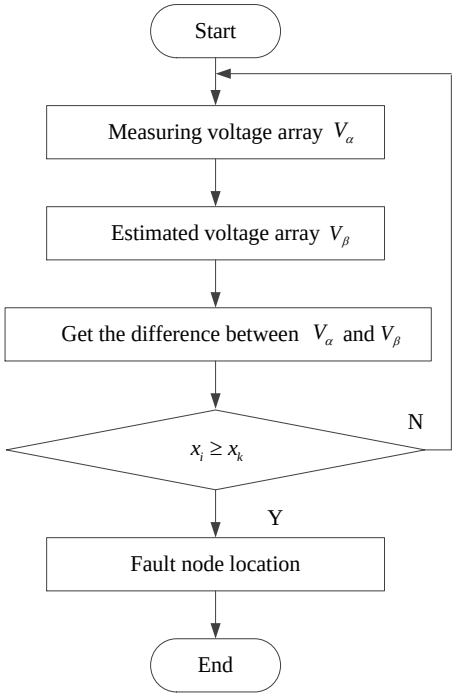

Fig. 2. Flowchart of fault node location.

C. Realization of Quantitative Security Protection for Distribution of Automation Nodes

1) Logical architecture and overall hardware structure of trusted power distribution terminal: In order to protect the nodes of the distribution network automation system, the trusted computing technology [11,12] is comprehensively used to design a trusted distribution terminal based on trusted computing, with access control as the core and security management as the support. The trusted power distribution terminal is based on the trusted platform of the hardware layer as the root of trust, and the trusted cryptographic module provides cryptographic computing services for the trusted computing platform. In order to give full play to the computing function of the trusted cryptographic module, it is also necessary to implement the trusted service management platform module based on the security protocol at the operating system layer. The logical architecture of the trusted power distribution terminal is shown in Fig. 3.

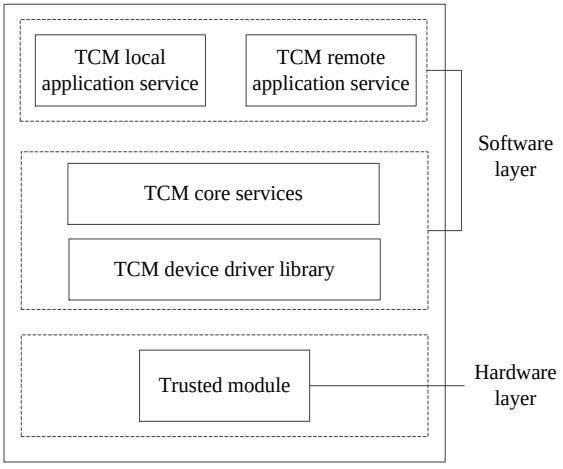

Fig. 3. Logical architecture of trusted power distribution terminal.

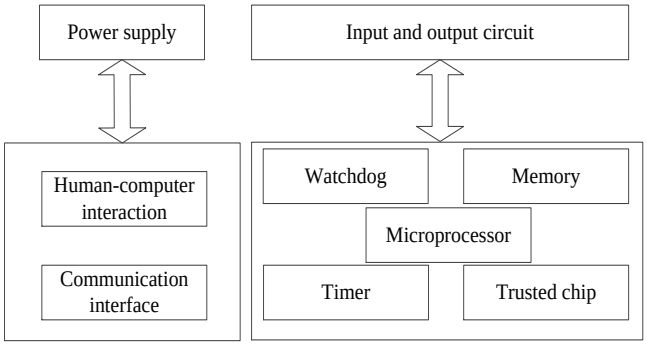

Fig. 4. Overall hardware structure of trusted power distribution terminal.

The overall hardware structure of the trusted power distribution terminal is shown in Fig. 4, which mainly includes microprocessors, human-computer interaction and communication interfaces [13,14]. The microprocessor consists of a watchdog, a memory, a timer and a trusted chip: the trusted chip is the core for realizing the trust and provides the root of trust for the trust chain; the memory is mainly responsible for the storage and memory functions; the timer realizes the timing and computing functions. The watchdog provides system resilience against transient failures [15-17]. The trusted control module is the core component of trusted computing. The root of trust is implanted inside to realize the root of trust control function, so as to combine password and control to realize active control and active defense of the nodes of the entire distribution network automation system. While measuring the mainboard controls, it also provides security computing capability support for the measurement mechanism of the software system.

2) Software design of trusted power distribution terminal: The distribution network automation system node is a device that can operate and control independently in the distribution network automation system [18, 19]. It is the basic object of constructing the distribution network automation system. The logical architecture and overall hardware structure of the trusted power distribution terminal have been introduced above, and the following will focus on the analysis of the trusted power distribution terminal software.

The control function application interface is a bridge connecting the software system and the hardware platform. When the hardware layer is powered on, the trusted control module will measure the motherboard controls, and complete the hardware environment and configuration settings through secure boot, thereby establishing a trusted chain. Provide support and services for the software layer. While processing information flow and energy flow, nodes have different processing capabilities of information, so the specific implementation will be set according to the functional requirements of nodes.

Nodes usually perform denoising, compression and other processing operations on data, and these operations will be recorded in PCR for metric protection. The node usually stores the collected data locally for a period of time, and then submits it to the superior node unit, or submits it to the superior node unit in time; therefore, data information storage is very important. For a small amount of collected data d, this paper adopts the domestic SM2 asymmetric encryption algorithm [20], and the encryption method is expressed as:

$$d_s = \omega_{TCM}\left(d, \theta_{PCR}, \mu_d\right) \tag{14}$$

In the formula: d_s is data encryption; ω_{TCM} is TCM algorithm; θ_{PCR} is the expected value of PCR, only when the expected value can be decrypted; μ_d is the node encryption public key. When the amount of data is large, the more efficient symmetric encryption algorithm SM4 is used, namely:

$$d_s = \omega_{SM4}\left(d, \theta_{PCR}, \mu_{SM4d}\right) \tag{15}$$

In the formula: ω_{SM4} is the SM4 encryption algorithm; μ_{SM4d} is the symmetric key.

When the system needs to use data, it will first obtain the current PCR value of the system and compare it with the expected value. Only when the comparison result is consistent, it will use the key stored by itself to decrypt it, so as to ensure the integrity and confidentiality of the distribution automation system nodes, and thus realize the quantitative security protection of the distribution automation nodes.

IV. Experimental Verification Analysis

In order to verify the effectiveness and application effect of the distribution automation node quantitative security protection technology based on the attack tree, an experimental study is carried out.

The IEEE33 node standard distribution system with a voltage level of 10kV is selected as the analysis object. For the distribution network with multiple nodes, the method in this paper, the method in the literature [5] and the method in the literature [6] are used to carry out the quantitative safety protection test of the distribution automation nodes. In order to ensure the accuracy of the experimental results, MATLAB software is used to process the experimental results.

1) Fault node location effect: In order to verify the safety protection effect of the method in this paper, compared with the method of literature [5] and literature [6], the fault node location accuracy of the three methods is analyzed. The fault node location accuracy will have a certain impact on the quantitative safety protection of distribution automation nodes. The higher the accuracy of fault node location, the better the quantitative safety protection effect of distribution automation nodes. The specific experimental results are shown in Fig. 5.

2) Time-consuming test of trusted computing: Secondly, it is time-consuming to test the trusted computing of the method in this paper, the method in the literature [5] and the method in the literature [6]. The test results are shown in Table I.

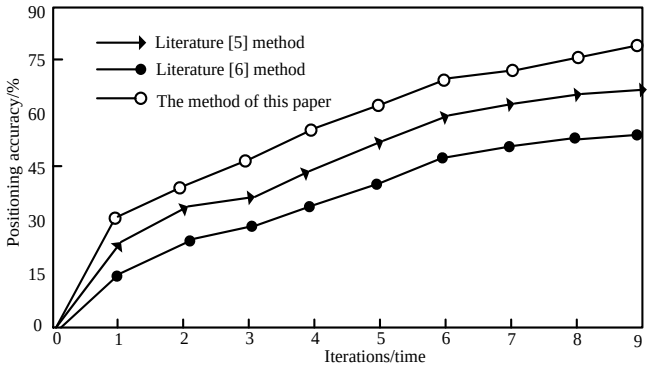

Fig. 5. Comparison results of fault node location accuracy.

TABLE I. TRUSTED COMPUTING TIME-CONSUMING TEST RESULTS/S

Iterations/time	The method of this paper	Literature [5] method	Literature [6] method
1	3.62	5.21	4.32
2	3.70	5.30	4.52
3	3.84	6.26	5.24
4	4.25	6.68	5.97
5	4.29	7.19	6.32
6	4.40	7.24	6.65
7	4.54	7.85	7.57
8	5.62	8.54	7.85
9	5.85	9.25	9.25

3) Network robustness test of distribution network automation system: Finally, the robustness of the distribution network automation system network is tested under the condition of increasing number of fault nodes. The specific test results are shown in Fig. 6.

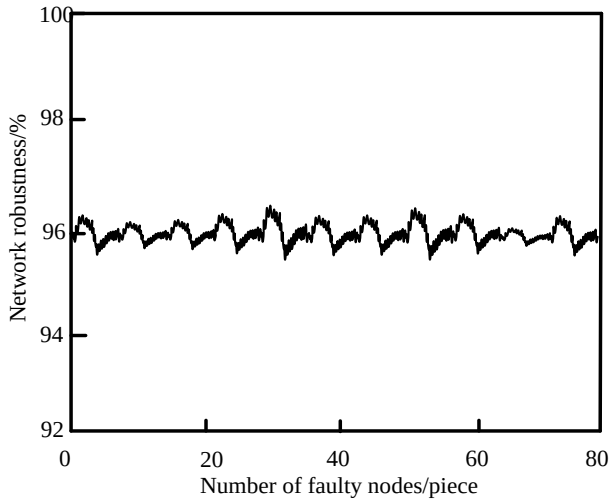

Fig. 6. Network robustness test results.

V. DISCUSSION

The effectiveness of the design method has been experimentally analyzed in the previous section, and the following conclusions can be drawn:

1) It can be seen from Fig. 5 that the node positioning accuracy of the distribution network automation system of this method is the highest among all methods. With the continuous increase of the number of iterations, the fault node positioning accuracy curve continues to grow, and the highest value of the fault node positioning accuracy reaches more than 80%, which shows that the method in this paper has a good security protection effect of distribution automation node quantification. In contrast to the other two methods, although with the continuous increase of the number of iterations, the fault node location accuracy is gradually improved, but there is still a certain gap between the fault node location accuracy and the method in this paper. This is because the method in this paper analyzes the risk assessment factors of the nodes in the distribution automation system, and through the evaluation and analysis of node vulnerabilities, the fault nodes in the distribution automation system are found in advance, so as to improve the positioning accuracy of the fault nodes.

2) According to the data in Table I, the method in this paper, the method in literature [5] and the method in literature [6] have a certain increase in the time-consuming of trusted computing in the process of increasing the number of iterations, but the overall increase in the method in this paper is small, indicating that the trusted computing efficiency of the method in this paper is high, and the minimum trusted computing time is only 3.62s, which shows that the quantitative security protection of the distribution automation nodes of the method in this paper is faster, which is beneficial to improve the security of the power system. This is because the design method took the lead in analyzing various factors and carried out analysis on the basis of grasping the overall factors, thus reducing unnecessary time waste and improving efficiency.

3) According to the network robustness fluctuation test results in Fig. 6, it can be found that after the number of fault nodes increases, the robustness of the distribution network automation system network does not fluctuate greatly, and the overall fluctuation has certain regularity, which indicates that the security protection effect of this method is good, and the network attack cannot be cracked. This is because this method uses trusted computing technology to design trusted distribution terminals. When the amount of data is large, a more effective symmetric encryption algorithm SM4 is required, which can better achieve the node security protection in the distribution automation system.

VI. CONCLUSION

In order to improve the security of distribution automation system nodes and ensure the safe operation of the distribution network as the research goal, a quantitative security protection technology based on attack tree for distribution automation nodes is proposed. Analyze the factors of node risk assessment of the distribution automation system, evaluate the node vulnerability of the distribution automation system, and comprehensively assess the risk of the distribution automation system using the attack tree. According to the evaluation results, the distribution network control model under network attack is constructed, the fault node is located, and the trusted distributed terminal is designed using trusted computing technology to achieve the node security protection of the distribution network automation system. The research results show that the fault node location accuracy of the method in this paper is high, the maximum fault node location accuracy is more than 80%, the trusted computing time is low, and the minimum trusted computing time is only 3.62 seconds. Moreover, the robustness of the system network fluctuates little, and the overall fluctuation has certain regularity, which shows that the method has certain effectiveness, and has certain application value and advantages in this field. However, as other performance indicators were not analyzed in the analysis process, there may be some deficiencies, which will become the focus of the next study.

ACKNOWLEDGMENTS

The study was supported by “Research and Development of Key Technologies for Safety Protection of Power Distribution Automation System Based on Electric Power Industrial Control Safety Shooting Range (Grant No. B311NB220002)”.

REFERENCES

[1] Lin Y J, Jing C, Cao C, Bai K. Distributed Power Supply Access Distribution Network Planning with Timing Characteristics. Computer Simulation, 2022, 39(2):51-55,72.

[2] Xie L, Luo L, Li Y, Zhang Y, Cao Y. A Traveling Wave-Based Fault Location Method Employing VMD-TEO for Distribution Network. IEEE Transactions on Power Delivery, 2020, 35(4):1987-1998.

[3] Bhagavathy S, Pearsall N, Putrus G, Walker S. Performance of UK Distribution Networks with single-phase PV systems under fault. International journal of electrical power and energy systems, 2019, 113(12):713-725.

[4] Chen K, Hu J, Zhang Y, Yu Z, He J. Fault Location in Power Distribution Systems via Deep Graph Convolutional Networks. IEEE Journal on Selected Areas in Communications, 2020, 38(1):119-131.

[5] Ni W D, Wu L H, Wang J F. Cyber security protection and hardware acceleration of distribution automation system based on autonomous security chip. Journal of Electric Power Science and Technology, 2020,35(03):166-172.

[6] Wu J Y, Chen H Q, Zhang L J, Lai Y Y. Research on Information Security Protection of Active Distribution Network Based on Trusted Computing. Guangdong Electric Power, 2020,33(03):79-87.

[7] Shameem M, Khan A A, Hasan M G , Akbar M A . Analytic Hierarchy Process Based Prioritisation and Taxonomy of Success Factors for Scaling Agile Methods in Global Software Development. IET Software, 2020, 14(4):389-401.

[8] Yang L G, Li C, Lu L, Guo T. Evaluation of port emergency logistics systems based on grey analytic hierarchy process. Journal of Intelligent and Fuzzy Systems, 2020, 39(3):4749-4761.

[9] Buldas A, Gadyatskaya O, Lenin A, Mauw S, Trujillo-Rasua R . Attribute evaluation on attack trees with incomplete information. Computers & Security, 2020, 88(1):101630.1-101630.17.

[10] Abdo H, Kaouk M, Flaus J M, Masse F. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie -combining new version of attack tree with bowtie analysis. Computers & Security, 2018, 72(1):175-195.

[11] Ibrahim F, Hemayed E E. Trusted Cloud Computing Architectures for infrastructure as a service: Survey and systematic literature review. Computers & Security, 2019, 82(5):196-226.

[12] Yoro R E, Ojugo A A. An Intelligent Client-Trusted and Dependable Security Framework to Ease Smartphone Portability on Community Cloud-Computing. Computer Networks, 2019, 6(1):1-7.

[13] Zou X F, Xiao Y X. Modbus telegram security of distribution network based on SM2. Power System Protection and Control, 2018, 46(12):151-157.

[14] Chen W, Xue H, Wang T Y, Cui J S, Wang L N. Olympic:A Data Symmetric Encryption Algorithm Based on Multiple Plaintexts. Journal of Wuhan University(Natural Science Edition), 2021, 67(3):213-220.

[15] Li T, Wang G, Liu Y, Yang Z B, Ren S, Shang W L. Information Security Risk Analysis of Intelligent Terminal in Distribution Network. Smart Power, 2020, 48(9):118-122.

[16] Li Hongxin, Zeng Jiang, Zhang Huaying, et al. Voltage sag analysis of a transmission and distribution network based on a compensation method under a distribution network fault. Power System Protection and Control, 2020, 48 (16): 45-53.

[17] Sun Yangsheng, Tu Qi, Huang Zhenyu, et al. Intelligent transmission technology of fault information in a resilient distribution network based on 5G and IEC61850. Power System Protection and Control, 2022, 50 (21): 108-117.

[18] Miao Renjie, Liu Yulin, Zhang Li, et al. A Fault Location Algorithm in Radial Distribution Networks with Distributed Generators Based on Multi-Agent Technology. Power System and Clean Energy, 2021, 37 (01): 8-15.

[19] Li Zhenxing, Xu Hao, Fu Yuting, et al. Fault Identification Strategy for Distribution Network with DGs Using Current Cosine Similarity. Proceedings of the CSU-EPSA, 2022, 34 (4): 1-10.

[20] Li Jiawei, Wang Xiaojun, He Jinghan, et al Distribution Network Fault Location Based on Graph Attention Network. Power System Technology, 2021, 45 (6): 2113-2121.