Journal of Organizational and End User Computing
Volume 33 • Issue 6 • November-December 2021

Self-Organized Network Management and Computing of Intelligent Solutions to Information Security

Xiaomeng Zhu, School of Public Administration, China Hohai University, China

ABSTRACT

The network in the information age has become an important part of life, but in the process of in-depth application of computers and networks, information security issues have also become a significant obstacle to their development. The intelligent solution to information security is a self-organized management and computing security protocol that is completed through the intelligent technologies at both ends of the sensing device and network authentication center. The results show that the network security information communication and publicity management platform built by the self-organized network management and computing of the intelligent solutions to information security can effectively heighten network user awareness of information protection, enhance the security of network environment, and promote the improvement of scientific network security rules. The study results of this paper provide a reference for further studies on self-organized network management and computing of intelligent solutions to information security.

KEYWORDS

Information Security, Intelligent Solutions, Network Computing, Self-Organized Network Management

1. INTRODUCTION

The information age has arrived, and network has become an important part of life. However, in the process of in-depth application of computers and networks, information security issues have also become a significant obstacle to their developments. Computer viruses, leakage of confidential information, hacker intrusion, and other issues have caused the economic and property losses of network users, and have negatively affected people's normal lives (Carvalho et al., 2016). Therefore, the search for intelligent solutions to information security has become one of the important contents of network development. In the new era of continuous development of intelligence, the network security monitoring and information network technology must be good at combining and using the results of intelligent advantages to improve the level of network security monitoring and self-organized network computing, and then provide more comprehensive services when involved in information security (Salem & Ali, 2020). Message security is also information security, which means that data packets communicated and transmitted in the network must satisfy data confidentiality, integrity, authenticity, and freshness. Message security is the basic requirement and the primary task to ensure the security of wireless sensor networks (Utkin et al., 2017). Generally, encryption, decryption and authentication mechanisms are used to ensure message security and the realization of network security mainly relies on computer information management technology. Through the management of network

DOI: 10.4018/JOEUC.20211101.oa28

applications, problems and security risks in the process of network applications can be discovered in time (Rahim & Javed, 2017).

In the process of information use, due to the characteristics of self-organized network computing outsourcing, the entire information retrieval and acquisition process is performed in the cloud and the cloud server can completely control the entire retrieval process and determine the final return result (Pham et al., 2019). The information user will not be possible to directly verify the completeness and correctness of the information returned by the cloud server. At the same time, in order to protect its own efficiency, intelligent solutions may not actively report the incorrect modification or deletion of information to the information owner, and in an environment of credibility competition, intelligent solutions can be used by manipulating information process to maximize benefits (Burtsev et al., 2017). In the specific network, attackers can be divided into external attackers and internal attackers and an external attacker is a powerful attacker who can observe and analyze all traffic in the specific network (Talabeigi & Naeeini, 2016). Because external attackers are not part of the system, they do not have the key of the entire system and cannot decrypt and sign messages, but they can obtain relevant information and use it for traffic and information analysis. Authorized and unauthorized information users are semi-trusted, which means that they will try their best to obtain some sensitive additional information from the query results and evidence (Ajulo et al., 2018).

Basis on the summary and analysis of previous research results, this paper expounded the research status and significance of intelligent solutions to information security, elaborated the development background, current status and future challenges of self-organized network management and computing, introduced the methods and principles of the network trust model and security reasoning mechanism, constructed the self-organized network management structure and scheme for the intelligent solutions to information security, proposed the self-organized network computing approach and framework for the intelligent solutions to information security, and finally conducted a simulation experiment and its result analysis. The study results of this paper provide a reference for further researches on self-organized network management and computing of intelligent solutions to information security. The detailed chapters are arranged as follows: Section 2 introduces the methods and principles of the network trust model and security reasoning mechanism; Section 3 constructs the self-organized network management structure and scheme for the intelligent solutions to information security; Section 4 proposes the self-organized network computing approach and framework for the intelligent solutions to information security; Section 5 conducts a simulation experiment and its result analysis; Section 6 is conclusion.

2. METHODS AND PRINCIPLES

2.1 Network Trust Model

For a network with a given network diameter a and average node moving speed b, the edge-added probability $Q(a, b)$ can be adjusted with reference to the following formula with the running time c:

$$Q\left(a,b\right)=\left(\frac{c}{d}\right)^{a_i}-\left(\frac{c}{e}\right)c^{b_i},i=1,2,\ldots,n \tag{1}$$

Where a_i is the shortest distance of node i in the certificate graph; b_i is the efficiency of node i exchanging certificate information; n is the number of network nodes; d is the initial set edge probability; e is the running time of the network.

The query operation performs the same hash mapping process, and then checks whether the corresponding bits are all ones. There is a false positive misjudgment when judging whether the element z belongs to the set; the following formula is used to express the false positive misjudgment rate W_j:

$$W_j = \sum_{j=1}^{m} \frac{a_j \log b_j}{\mathrm{k} \cdot \log\left[Q\left(a,b\right)\right]} \tag{2}$$

Where m is the number of elements in the real set; j is all network nodes in the simulation; a_j is the number of messages sent; b_j is the time to send the message; k is the check time of the list.

After each interaction is completed, the interaction nodes must give each other an evaluation, the satisfactory interaction evaluation is l, and the unsatisfactory interaction evaluation is m. In order to integrate the local trust value, the local trust value must be standardized. For this reason, the standardized local trust value $E(x)$ is calculated as follows:

$$E\left(x\right) = \sum_{x=1}^{n} o_x \left[l\left(x\right) - m\left(\bar{x}\right)\right] \tag{3}$$

Where x is the reputation evaluation value; $\bar{x}$ is the weighting coefficient of the node reputation value in the computing; o_x is the set of nodes that node x has traded and purchased from it.

Assuming that the network works periodically according to the number of rounds, one round of data defined as the edge node of the network is sent to the sink node. In a round of monitoring period, a total of p data packets are received in the area, q is the node forwarding rate of the round, and the total forwarding rate $f(p)$ of the area from the beginning of work to the round:

$$f\left(p\right) = \frac{\left|W_j\left(p\right) - \overline{W}_j\left(p\right)\right|}{\left|E\left(p\right) - \overline{E}\left(p\right)\right|} \tag{4}$$

Each service evaluation of the network node is weighted and updated, so that the service evaluation of the node becomes stable and the continuous evaluation is combined, which not only reduces the load pressure of the node, but also makes the service of the node in the evaluation update, which provides for the selection of data sharing nodes. With reference to the basis, the probability $g_i(x)$ of the node's delay in the service process is:

$$g_i\left(x\right) = \sqrt{x_i\left(\frac{s}{q_i - x_i} - \frac{t}{r_i - x_i}\right)} \tag{5}$$

Where x is the time period; x_i is the number of node services; q_i is the number of delayed services; r_i is the data integrity; s is the data security; t is the service evaluation.

2.2 Safety Reasoning Mechanism

If all the experiences of X to Y are positive experiences, then X has a direct security relationship with Y; if X is willing to accept the experience of the target entity provided by Y, then X has a recommended security relationship with Y, then direct security X and indirect security in the computing formulas of Y is:

$$Z\left(X,Y\right)=u^2\sum_{i=1}^{n}\frac{v_i^2-w_i^2}{n-i} \tag{6}$$

Where u is the number of positive experiences obtained by X about Y; v is the possibility that X expects Y to successfully complete a task; w is the final recommendation entity on the recommended path; i is the trust degree derived from a single recommended path; n is the recommended limit of the number of layers.

In the trust model, some nodes may be unwilling to provide feedback to other nodes, so an incentive mechanism is needed to provide power for node evaluation. The network information security factor can act as an incentive factor to reward nodes that provide feedback and the basic trust value computing model is:

$$R_{ij}=\frac{1}{2n}\left[\sum_{i=1}^{n}\sum_{j=1}^{m}\frac{a_{ij}\left(b_{ij}-c_{ij}\right)}{d_{ij}\left(e_{ij}-f_{ij}\right)}\right]^{\alpha-1} \tag{7}$$

Where a_{ij} is the trust value between nodes i and j; b_{ij} is the number of transactions between nodes i and j; c_{ij} is the number of transactions between node i and all other nodes; d_{ij} is the interactive node during the i-th transaction of the node material; E_{ij} is the evaluation of the other party after the j-th transaction of node i; the credibility of the feedback provided by f_{ij} node i; α is the transaction context factor.

For a network information source with a node of m, the average speed of information circulation is denoted as s_i, the information density is denoted as t_i, the correction coefficient is denoted as u_i, and the network information communication distance is denoted as k_i, then the network delay T_i on the road section is:

$$T_i\left(x_i\right)=\begin{cases}\dfrac{1}{m-1}\lim\limits_{i\to 0}\dfrac{t_i-u_i}{s_i}\, i\neq m\\ \lim\limits_{i\to 0}\dfrac{t_i-k_i}{s_i}\, i=m\end{cases} \tag{8}$$

This formula shows that when the average distance between network nodes is less than or equal to m, data packets can be transmitted directly, and the delay i is proportional to the number of nodes. When the average distance is greater than m, information carrying data packets are required to achieve intermittent transmission.

Suppose the scale of network A is B, and the members move freely in the network, then the connection probability between nodes is d_i and the node degree is g_i. According to the random graph theory, in order to ensure the connectivity of the network, the connection probability P (A, B) between nodes is:

$$P\left(A,B\right)=\frac{\gamma}{\rho}\cdot\frac{d_i-l_i}{g_i-c_i} \tag{9}$$

Where l_i is the secret value of the node; c_i is the number of identity certificates owned by each node; γ is the probability of a certain secret value in the same set; ρ is the number of edges in the network.

The data acquisition module regularly obtains the specified network link state parameters, obtains the current network operating status E, transposes E, and converts it into network state information:

$$F = P\left(A, B\right) - Z\left(X, Y\right) \tag{10}$$

For most of the status attribute parameters, the timing polling strategy is used to obtain status information: for similar attributes, real-time collection is adopted, that is, the information is obtained in real time when the fault diagnosis operation is implemented. This is because they only pay attention to the network equipment in the diagnosis, regardless of its historical response characteristics.

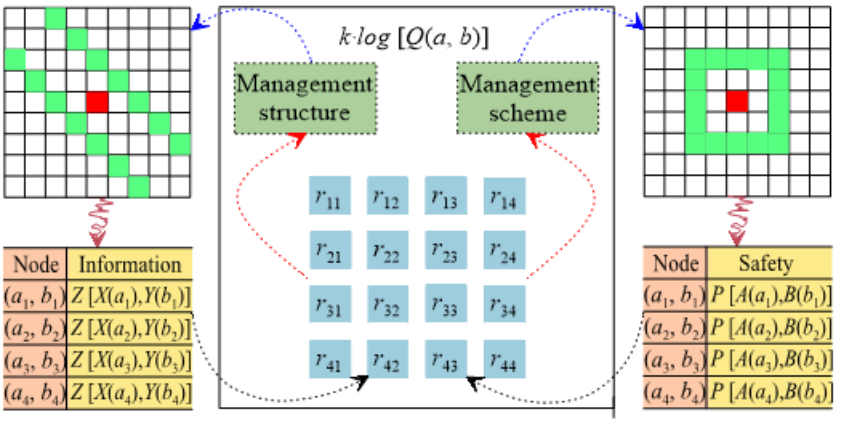
3. SELF-ORGANIZED NETWORK MANAGEMENT OF INTELLIGENT SOLUTIONS TO INFORMATION SECURITY

3.1 Self-Organized Network Management Structure

The security protocol is completed in the intelligent solution at both ends of the sensor equipment and the network authentication center. It is a self-organized and managed security protocol, and the cryptographic algorithm, key and security protocol software and data are stored in the intelligent solution at both ends In this way, the security level of the network-aware layer encryption system and security protocol is improved. The intelligent solution solves the problem of single-key cryptographic algorithm in the key update management of sensor equipment authentication, or signature and encryption protocol, reduces the cost of single-key update maintenance. At the same time, it exerts the speed of single-key cryptographic algorithm encryption and the advantage of fast speed effectively improves the operating efficiency of the network-aware layer security protocol. The intelligent solution analyzes the performance of network computing, and proposes that only lightweight encryption technology can be used in network computing embedded in network sensor equipment to establish a security protocol at the network perception layer, and a secure single-key management technology is used to solve the problem (Wang, 2020). The key update problem of lightweight ciphers is to realize the establishment of the sensor device authentication protocol, signature and encryption protocol on the sensor device side in the network computing of the network sensor device side (Figure 1). This solution establishes the authentication protocol, decryption, and signature verification protocol of the sensor device at the authentication center end in the encryption card chip of the network authentication center, and ensures that the sensor device at the network perception layer is credible, authentic, and has not been replaced.

Data loss is the main type of network security problem and the main purpose of hacker attacks. In response to such problems, measures such as data encryption, data selection, and related process encryption are adopted to prevent data loss. Network leaks often occur on the Internet, and data confidentiality has become a key issue in network information management. Carrying out a security risk assessment for the information resources of the information scheme is of great significance to building a security assessment protection system, improving the assessment mechanism, and filling security vulnerabilities. The management activities in specific work are affected by various factors, and it is difficult to find problems in network information management in time. Network information technology has been widely used in companies, but there are still many problems in implementing network information security management. The establishment of a network security assessment mechanism mainly implements pre-assessment, mid-event assessment and post-event assessment. Computer information management technology is used to build a security assessment system to find out the root cause of network security problems in the scheme, and scientifically analyze the response

Figure 1. Self-organized network management structure of intelligent solutions to information security



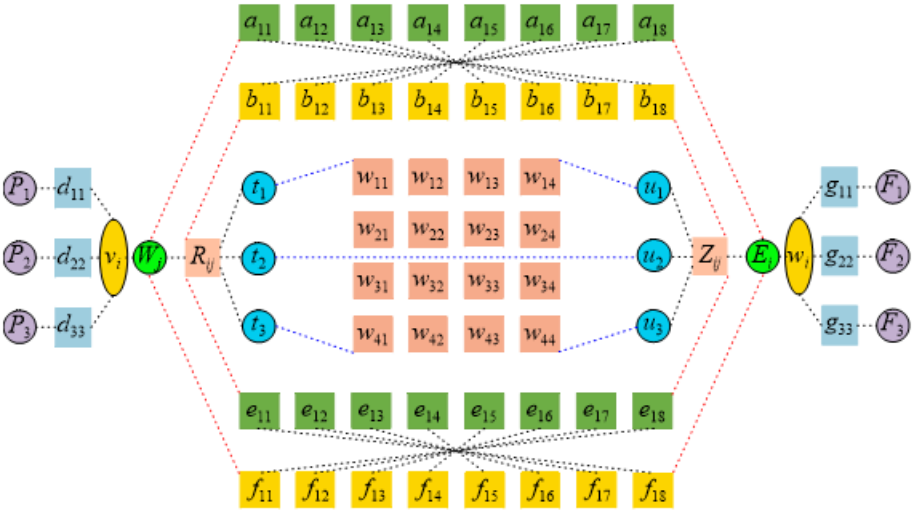
mechanism to improve the security of the network system protection ability. The self-organization and management of the network builds a network security information communication and publicity management platform, which can effectively improve people's protection awareness, enhance the security of the network environment, and promote the establishment of scientific network security rules (Utkin et al., 2017).

The topology of the specific network is dynamic and changes at any time. This means that information security must have the ability to respond quickly to topological changes, converge quickly when computing the scheme, and obtain an effective scheme in time to avoid the occurrence of destination nodes. However, in a specific network, due to the dynamic change of the topology, a large amount of existing scheme information will be invalidated in a short time, which makes it easier to produce scheme loops. Therefore, in specific networks, it is particularly important and more difficult to provide a loop-free solution. In the intelligent solution of information security, each node in the network periodically sends the latest scheme information to other nodes, and each node must save one or more scheme tables to store the scheme information. When it is not possible to encapsulate all the program update entries in the program update list in one program update message and send it at one time, the program update list will be divided into multiple parts and be encapsulated in multiple program update messages and sent several times. When the network topology changes, nodes broadcast program update messages in the entire network, so that each node can continuously obtain network information. When the neighbor node receives the scheme information table containing the modification, it first compares the scheme sequence numbers of the source node and the destination node. The scheme information with a larger serial number is always received, and the scheme with a smaller destination node's serial number is eliminated.

3.2 Self-Organized Network Management Scheme

Once information security has carried out the centralized management of self-organized network, it is necessary to carefully evaluate how the data is accessed, stored and used. These schemes save data on the server side through intelligent solutions without leaving any traces on physical mobile devices. At the same time, any data input and output devices need to be highly encrypted, and information security needs to be able to control whether files can be deleted, restored, modified or shared, no matter where the data information exists or how it is used. These intelligent solutions belong to network computing, and cannot be compared with traditional information security solutions in terms of security and manageability (Figure 2). They cannot provide ordinary employees with assistance in the installation, maintenance and repair of personal equipment through self-organized network

Figure 2. Self-organized network management scheme of intelligent solutions to information security



and management. Managers don't even know where these unfamiliar devices come from and their management link often lacks the ability to conduct risk assessment of internal mobile devices, which intensifies the difficulty of handling security issues. This requires that the management link must distinguish the security of network computing, define and strengthen mobile security policies, in order to maintain the balance between information circulation and security. At the same time, self-organized network management also needs to consider how to achieve a balance between the privacy protection of organizations and individuals. While protecting the data resources of the organization, ensure the privacy of users' personal information.

Each node in the network maintains a neighbor node table at the same time to record the neighbor node of each node and the remaining energy information corresponding to each neighbor node. If a neighbor node message is not received within a certain period of time, it is considered that the node has moved out of its communication range, it is deleted from the neighbor table, and the corresponding record is deleted in the pheromone table. The task of the path search phase is to find the best path between the source node and the destination node, and the task of the data packet forwarding phase is to send the data packet to the destination node according to the best path (Al-Shawabkeh et al., 2017). The survival time of the entire mobile specific network is an important indicator for judging the performance of the network. Extending the survival time of the network and strengthening the stability of network routing have become a question that must be considered in the routing design of the mobile specific network. Information security management control is the second level of the information security management system. Its purpose is to control and manage information security risks by improving the organizational structure, clarifying the positioning and responsibilities and mutual relationships of different security organizations and different security roles. Self-organized network computing takes appropriate corrective and preventive measures to identify and effectively implement an improved information security management system. Communicate the results and activities and consult with all relevant parties to revise the information security management system when necessary.

Self-organized network computing is to modify the configuration in the registry, which uses its own more complete management organization method to manage and configure the settings in various objects. It is far more convenient, flexible and more powerful than manually modifying the registry. Many configurations can be customized, but these configurations are published in all corners of the

registry. If it is manually configured, manager can imagine how difficult and complicated it is. This signature first encrypts the message digest with the sender's private key, and then sends it together with the original text to the recipient. The recipient can only use the sent public key to unlock the password (Shantharama et al., 2018). After decryption, those schemes use the generated the summary information is compared with the summary information of the decryption itself. The main function of self-organized network management is to control which users can log in to the server and obtain network resources, as well as control the time when users are allowed to access the network and which workstations are allowed to access the network. The identification and verification of the user name, the identification and verification of the user password and the default restriction check of the user account are the three steps of the user's network access control. As far as the three levels are concerned, if one of them fails to pass each other, it is difficult for the user to access the computer network used.

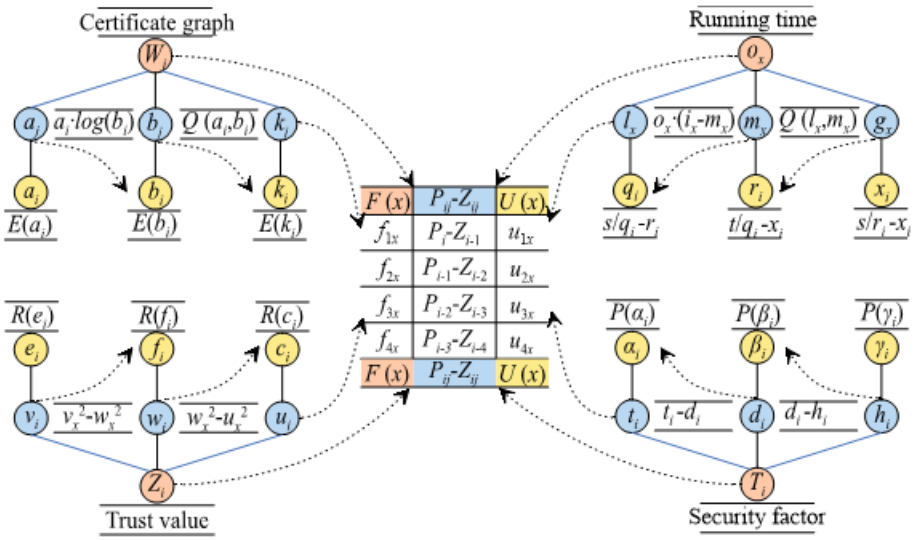
4. SELF-ORGANIZED NETWORK COMPUTING FOR INTELLIGENT SOLUTIONS TO INFORMATION SECURITY

4.1 Computing Recommended Approach

The establishment of trust relationship comes from the interaction of nodes with each other, and the result of the interaction becomes an important data source for trust evaluation, which can be forwarding data from the network layer, routing monitoring data, observation data, various security service data and various application transactions evaluation result. The basic trust value indicates the degree of trust that the subject establishes in the object at a certain moment in a given context. It can use the intermediate results of existing schemes, such as the success rate of interaction, the success rate of data forwarding, or the probability of the subject taking a certain action against the object. After the network has been running for a period of time, a node will hold some certificates of nodes far away from itself. These certificates represent a direct trust relationship, which acts as a shortcut and greatly improves the key authentication success rate (Figure 3). In the past, the issuance of certificates was mostly carried out by manual intervention between neighboring nodes within the physical security communication range of each other. The certificate issuance mode between cluster heads allows non-neighbor nodes to issue certificates, and the cluster heads are not necessarily in the physical security communication range of each other, which requires corresponding authentication measures to ensure the reliability of certificate issuance. No shortcut can be established between two cluster heads without any trust relationship; the certificate chain can be obtained through the recommendation of other nodes (Namasudra & Roy, 2018).

The mobile node in the intelligent solution is the network. In addition to the information related to the current network information security status, the information inside the network also involves the user's private information such as user identity information, network static information, network dynamic information, personalized service requirements, etc. Therefore, the protection of the privacy information of these mobile nodes should be considered during information transmission. In the self-organized network management, the attacker intercepts the message transmitted in the communication channel by eavesdropping, etc., and then repeatedly sends the information to the entity in the same way. It can be the original target user or other entities. The recipient thinks it is sent by a legitimate user, which confuses the traffic information that should be received at present and even misjudgments. When designing a security protocol, manager can defend against such attacks by means of timestamps or random values. If conventional solutions may cause the leakage of private and secret information, attackers can use the secret information to illegally access resources and services, or pretend to be legitimate users to send false messages to the solution, posing a threat to the entire network. Attackers use node capture attacks to obtain secret information such as keys stored in nodes, and subsequently pretend to be legitimate nodes to send false information to the network, causing major security risks.

Figure 3. Computing recommended approach for intelligent solutions to information security

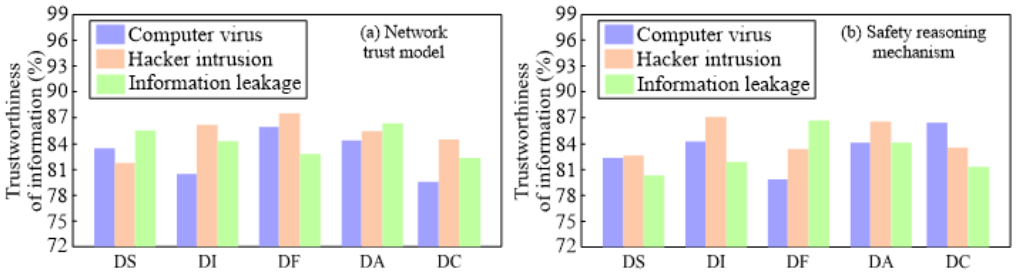


The data resource layer mainly includes real-time log data collected by network information security equipment and various knowledge data for network information security decision-making. The real-time log data mainly includes log data such as online behavior management system, application firewall, bastion host, etc., which are stored in a relational database after standardized processing. Knowledge data mainly includes network information security event rule characteristics, protection rules, and daily processing knowledge data. After ontology description and self-organization management are integrated, they are stored in the self-organization management database (Ahmed, 2017). After the network information security ontology is constructed, it is necessary to create some test cases for the constructed ontology, and use the test examples to detect whether the constructed ontology model achieves the expected purpose and whether the constructed network information security ontology model has errors. The user interface layer is mainly composed of two functional modules: intelligent solution requirement input and decision result display. The user inputs the decision requirements through natural language, and then the system begins to analyze and calculate the requirements, and after the decision results are obtained, the decision results are displayed in the form of tables and graphs. The system can not only provide decision support information when the self-organized network computing makes a request, but also can set a push strategy in advance to actively push some decision-making conclusions to relevant personnel.

4.2 Computing Clustering Framework

The information in the self-organization of the network can realize the message sharing between the information through network communication, and the information can obtain the status of the intelligent scheme in advance, and take effective measures to avoid scheme risks and avoid scheme congestion. Through the communication with roadside base stations, the scheme management department can obtain massive scheme information. Through the analysis of this information, the scheme management department can understand the real-time scheme status and formulate effective strategies to command the scheme. Improve the efficiency of the management department (Shrimali, 2017). Malicious attackers in the self-organized network of the network obtain network information in the network by using some monitoring equipment, obtain the identity of the user through the analysis of these messages, and pretend to be a legitimate user to spread false messages. Trustworthiness of

Figure 4. Trustworthiness of information of different data parameters with computer virus, hacker intrusion, and information leakage in the network trust model (a) and safety reasoning mechanism (b); Note: DS-Data security; DI-Data integrity; DF-Data freshness; DA-Data authenticity; DC-Data confidentiality

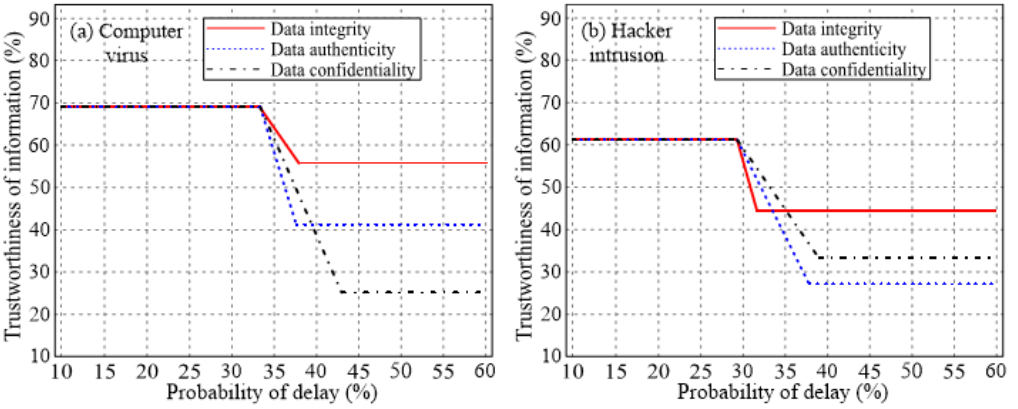


information of different data parameters with computer virus, hacker intrusion, and information leakage in the network trust model and safety reasoning mechanism are shown in Figure 4. For example, the attacker spreads false news to make other nodes mistakenly believe that the scheme ahead is congested, and then choose other schemes, so that the malicious attacker can make his smart scheme more smooth, but it does cause losses to other nodes, and it greatly aggravates them. For this kind of attack, a secure authentication protocol should be used. The legitimate node can distinguish whether the sender of the message is a legitimate user and whether the message is reliable through message authentication.

The policy-based self-organized network management technology mainly provides a standard and general mechanism for standardizing applied security policies and credentials, and unifies security policies, credentials, access control and authorization. Policies and credentials written in standard languages can be interpreted by all self-organized network management applications. The self-organized network management strategy is easy to distribute through the network, and can avoid the use of specific application-specific distributed policy configuration mechanisms, access control lists, certificate analysis, etc. Compared with traditional identity-based access control systems, this type of system unifies the two concepts of identity authentication and authorization, and simplifies complex authorization judgments. The main basis for evaluating the direct trust relationship comes from direct interactive experience information; the trust transfer between entities is mainly manifested in the transfer and adoption of recommended information. Recommendation trust is the degree of trust that an entity has for the recommendations provided by another entity and all of them involve subjective judgments (Dagher et al., 2018). During the operation of the self-organized network management system, it is inevitable to check whether the user certificate and the trust relationship asked by the user comply with the local security policy. This is one of the core issues of the self-organized network management. At present, research in this area has achieved certain results, but there is still a need for a more complete consistency check algorithm in terms of safety, efficiency, and practicability. Figure 5 shows the trustworthiness of information of different probabilities of information delay with computer virus and hacker intrusion

In the application of network information security management technology, the security of the operating system is a key part and it plays a very important role in normal operation. Therefore, it is necessary to strengthen the security protection of the network operating system to ensure the normal operation of the computer. For example, establish a computer security protection system, check some security problems and security vulnerabilities in the operating system, and solve them in time to avoid the invasion of various viruses to the greatest extent. At the same time, it can also use firewalls, intrusion detection software, etc. for further protection, improve operating system logs, predict and analyze the security that may occur in the network, and take preventive measures (Li et al., 2016). The purpose of self-organized network computing is to establish an information security

Figure 5. Trustworthiness of information of different probabilities of information delay with computer virus (a) and hacker intrusion (b)



management mechanism and operation mode centered on the internal users of the organization, using a new set of methods to comprehensively and centrally manages the infrastructure of intelligent solutions. According to the actual needs of the business, it is to provide information services with measurable costs and measurable quality to ensure stable and efficient business operations and achieve organizational goals. The platform's functions include fault management, performance management, security management, change management, problem management, release management, availability management, service level management, and configuration management.

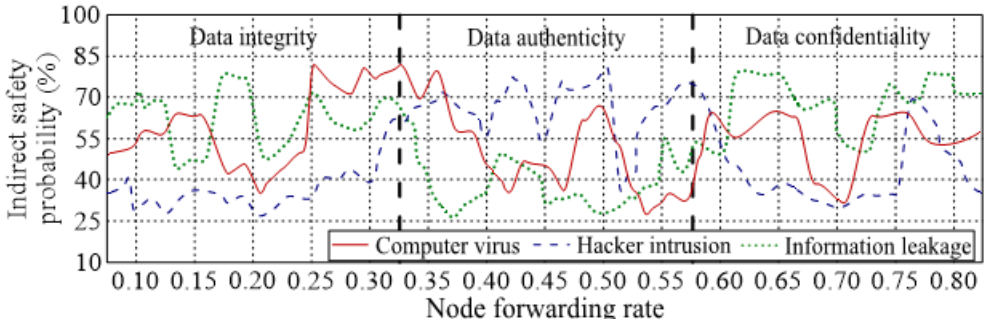
5. SIMULATION EXPERIMENT AND ANALYSIS

5.1 Simulation Experiment Design

Self-organized network computing nodes randomly select transmission objects, which will cause a large number of connections to be established between nodes that are far away from the network, thus making the average neighboring node distance longer. An ideal peer-to-peer network structure is that most of the connections are established inside the packets, so that nodes can obtain higher-quality transmission objects, and only a few connections are established between the packets, thus building two-layer network architecture. The upper layer contains for each group, the bottom layer contains the nodes in the group. When the newly joined node cannot find its own group in the network, it should create a new group by itself. This situation mainly occurs in the early stage of the establishment of a peer-to-peer network, at which time it will propose to the host to create its own group. In order to ensure the quality of service, the members in the adjacent group can be used for data transmission until the number of nodes in the group has met the data transmission requirements. When the master node list is large, the possibility of all failures is unlikely and the number of nodes in the newly created group is often small. If a group member node finds that all the nodes in the master node list are all failures, they can actively apply to the server and become the new master node to manage the group. With the help of the master node, each member of the group can obtain the information of all nodes in the group.

In the peer-to-peer network, a unified security management model is required to quantify the security value and establish a security relationship, so as to determine the interaction behavior based on the security relationship. Therefore, the rationality and effectiveness of the safety management model directly affect the stability and safety of the entire system. The security relationship between nodes is measured from the perspective of multiple attributes, and this security relationship is not

Figure 6. Indirect information safety probabilities of three typical network information security risks with different node forwarding rates



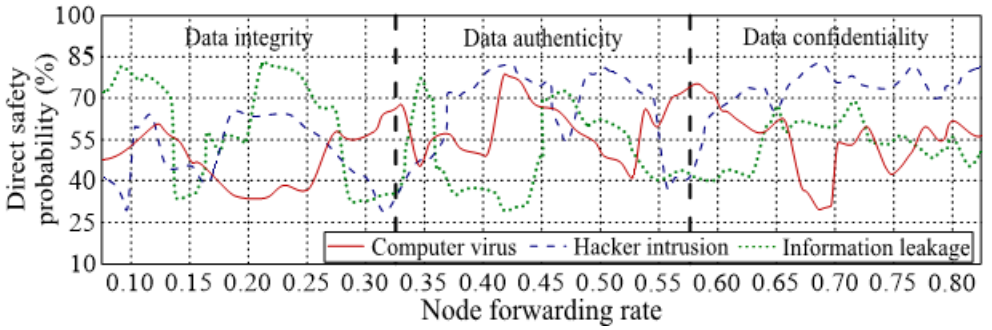
static, it will change with the interaction between nodes. How to reflect the uncertainty of the safety relationship and accurately calculate the safety value of the node is the main consideration of the safety management model. Therefore, many theories that have obvious advantages in dealing with the problem of information uncertainty have been applied to the information management model, and a large number of experiments have also proved that these theories can more optimize the security management model. By introducing risk assessment, the security model is more sensitive to malicious behaviors, and malicious nodes can be found faster, thereby reducing the losses caused by malicious transactions. On the other hand, the introduction of risk assessment is also a punishment mechanism for malicious behavior. Because the impact of malicious behavior has been considered when computing the direct safety value, the impact of malicious behavior is again considered when assessing the risk value, which can magnify the harm of malicious behavior. In this way, it is also in line with the characteristics of the safety value rising slowly and falling quickly.

5.2 Result Analysis

Information security awareness and self-organized network computing are important content in network security management, and their implementation will directly affect the degree to which network security policies are understood and the effect of being executed. Security management guarantees the integrity, confidentiality, and availability of network information assets by appropriately identifying information assets, evaluating the value of information assets, formulating and implementing security strategies, security standards, security policies, and security measures, and forming a network security culture through secure computing an important part of ensuring the smooth realization of safety management (Woo et al., 2016). They identify the information assets of the network, assess the risks that threaten these assets, and assess the disasters and losses that the network will endure if these risks become reality. Through various risk management methods such as reducing risks, avoiding risks, transferring risks, and accepting risks, it assists self-organized management to formulate network information security strategies. Figure 6 shows the indirect information safety probabilities of three typical network information security risks with different node forwarding rates. Network users can directly access the resources of the intelligent solution, which brings great convenience to the self-organization and management of the network; similarly, any user who can access the solution can also access the resources of the network, which has a great impact on the promotion of the network and the expansion of the network. There are benefits. With different network scales, business development, and security requirements, information security policies may vary, but security policies should be simple and clear, easy to understand, and directly reflect the theme, to avoid ambiguities (Zegzhda, 2016).

In order to prevent the message from being tampered, deleted, replayed and forged, an effective method is to make the sent message have the ability to be verified, so that the recipient or a third party

Figure 7. Direct information safety probabilities of three typical network information security risks with different node forwarding rates



can identify and confirm the authenticity of the message, and the password to achieve this kind of function The system is called an authentication system. The authenticity of the message is different from the confidentiality of the message. The confidentiality prevents the interceptor from deciphering the content of the cipher-text without knowing the key, while the authenticity prevents anyone who does not know the key from constructing a cipher-text. The recipient decrypts it into an understandable message and it is important to correctly set the validity period of the certificate when initializing and renewing the certificate (Zhang et al., 2019). The validity period of the certificate must be set so that the certificate can be updated regularly, which means that it must ensure that the node can join the network within the period of use to complete the creation of the updated certificate library. Figure 7 shows the direct information safety probabilities of three typical network information security risks with different node forwarding rates. The local certificate database search algorithm is relatively low in complexity due to its optimization characteristics, the algorithm complexity is relatively low, and the search of the certificate chain is only related to neighbor nodes, so the communication volume consumption is relatively low. However, when the number of nodes continues to increase, the communication consumption of the algorithm during the establishment of the authentication chain will also show a significant increase, indicating that the number of nodes has a great influence on the consumption of communication in the network (Hu et al., 2017).

The application range of self-organized network computing is very wide, but the common feature of traditional self-organized network computing applications is to collect the information collected by intelligent solutions. This requires a way to effectively collect and forward the information of intelligent solutions to The mechanism of assembling nodes. Traditional self-organized network computing faces many problems. Looking at the overall trend, as the number of network nodes increases, the connectivity of the network increases and the degree of congestion continues to increase, and the variability of the network topology decreases, so the end-to-end latency of information security decreases (Toch et al., 2018). In the self-organized network, each network is a node with complete information collection, processing, and wireless transmission functions, or in other words, each network is an intelligent sensing node. In the self-organized network, network nodes are used as intelligent solution nodes to collect road traffic information, and the organization constitutes a new type of self-organized network computing. In addition, self-organized network computing has characteristics that traditional intelligent solution networks do not have, including more sufficient energy for nodes in the network and stronger wireless transmission capabilities. At the same time, since the network nodes are always in a state of motion during the detection process, each node can collect road data more effectively.

6 CONCLUSIONS

This paper introduced the methods and principles of the network trust model and security reasoning mechanism, constructed the self-organized network management structure and scheme for the intelligent solutions to information security, proposed the self-organized network computing approach and framework for the intelligent solutions to information security, and finally conducted a simulation experiment and its result analysis. Self-organized network computing nodes randomly select transmission objects, which will cause a large number of connections to be established between nodes that are far away from the network, thus making the average neighboring node distance longer and the mobile node in the intelligent solution is the network. In addition to the information related to the current network information security status, the information inside the network also involves the user's private information such as user identity information, network static information, network dynamic information, personalized service requirements, etc. Therefore, the protection of the privacy information of these mobile nodes should be considered during information transmission. An ideal peer-to-peer network structure is that most of the connections are established inside the packets, so that nodes can obtain higher-quality transmission objects, and only a few connections are established between the packets, thus building two-layer network architecture. The upper layer contains for each group, the bottom layer contains the nodes in the group and self-organized network computing is to modify the configuration in the registry. It uses its own more complete management organization method to manage and configure the settings in various objects and it is far more convenient, flexible and more powerful than manually modifying the registry. The results show that the network security information communication and publicity management platform built by the self-organized network management and computing of the intelligent solutions to information security can effectively heighten network users' awareness of information protection, enhance the security of network environment, and promote the improvement of scientific network security rules. The study results of this paper provide a reference for further researches on self-organized network management and computing of intelligent solutions to information security.

REFERENCES

Ahmed, A. A. (2017). Investigation approach for network attack intention recognition. *International Journal of Digital Crime and Forensics*, *9*(1), 17–38. doi:10.4018/IJDCF.2017010102

Ajulo, E. B., Akinyede, R. O., & Adewale, O. S. (2018). Security threats and privacy issues in vehicular ad-hoc network (VANET): Survey and perspective. *Journal of Information*, *4*(1), 1–9. doi:10.18488/journal.104.2018.41.1.9

Al-Momani, A. M., Mahmoud, M. A., & Ahmad, M. S. (2018). Factors That Influence the Acceptance of Internet of Things Services by Customers of Telecommunication Companies in Jordan. *Journal of Organizational and End User Computing, 30*(4), 51-63.

Al-Shawabkeh, M. M. M., Saudi, M. M., Alwi, N. H. M., & Azman, N. (2017). Information security management systems (ISMS) and computer security self-efficacy (CSSE) model comparison. *Advanced Science Letters*, *23*(6), 5237–5241. doi:10.1166/asl.2017.7349

Burtsev, A. G., Klishevich, D. M., & Polyanskii, A. V. (2017). Protection of standard network protocols of automated production control systems. *Russian Engineering Research*, *37*(3), 224–232. doi:10.3103/S1068798X17030066

Carvalho, L. F., Barbon, S. Jr, Mendes, L. de S., & Proença, M. L. Jr. (2016). Unsupervised learning clustering and self-organized agents applied to help network management. *Expert Systems with Applications*, *54*, 29–47. doi:10.1016/j.eswa.2016.01.032

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, *39*, 283–297. doi:10.1016/j.scs.2018.02.014

Gonzales, D., Kaplan, J. M., Saltzman, E., Winkelman, Z., & Woods, D. (2017). Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds. *IEEE Transactions on Cloud Computing*, *5*(3), 523–536. doi:10.1109/TCC.2015.2415794

Hu, P., Ning, H., Qiu, T., Song, H., Wang, Y., & Yao, X. (2017). Security and privacy preservation scheme of face identification and resolution framework using fog computing in Internet of Things. *IEEE Internet of Things Journal*, *4*(5), 1143–1155. doi:10.1109/JIOT.2017.2659783

Li, S., Tryfonas, T., & Li, H. (2016). The Internet of Things: A security point of view. *Internet Research*, *26*(2), 337–359. doi:10.1108/IntR-07-2014-0173

Luna, J., Taha, A., Trapero, R., & Suri, N. (2017). Quantitative reasoning about cloud security using service level agreements. *IEEE Transactions on Cloud Computing*, *5*(3), 457–471. doi:10.1109/TCC.2015.2469659

Namasudra, S., & Roy, P. (2018). Ppbac: Popularity Based Access Control Model for Cloud Computing. *Journal of Organizational and End User Computing, 30*(4), 14-31.

Nugraha, Y., Brown, I., & Sastrosubroto, A. S. (2016). An adaptive wideband delphi method to study state cyber-defence requirements. *IEEE Transactions on Emerging Topics in Computing*, *4*(1), 47–59. doi:10.1109/TETC.2015.2389661

Pham, L. M. T., Tran, L. T. T., Thipwong, P., & Huang, W. T. (2019). Dynamic Capability and Organizational Performance: Is Social Networking Site a Missing Link? *Journal of Organizational and End User Computing, 31*(2), 1-21.

Rahim, A., & Javed, A. (2017). A special section on intelligent computing and network security in healthcare. *Journal of Medical Imaging and Health Informatics*, *7*(3), 653–654. doi:10.1166/jmihi.2017.2038

Salem, F. M., & Ali, A. S. (2020). SOS: Self-organized secure framework for VANET. *International Journal of Communication Systems*, *33*(7), 4317. doi:10.1002/dac.4317

Shantharama, P., Thyagaturu, A. S., Karakoc, N., Ferrari, L., Reisslein, M., & Scaglione, A. (2018). LayBack: SDN management of multi-access edge computing (MEC) for network access services and radio resource sharing. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 57545–57561. doi:10.1109/ACCESS.2018.2873984

Shrimali, S. (2017). DeMilitarized Zone: Network architecture for information security. *International Journal of Computers and Applications*, *174*(5), 16–19. doi:10.5120/ijca2017915389

Talabeigi, E., & Naeeini, S. G. J. (2016). Information security risk management and incompatible parts of organization. *Journal of Industrial Engineering and Management*, *9*(4), 964–977. doi:10.3926/jiem.2032

Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The privacy implications of cyber security systems: A technological survey. *ACM Computing Surveys*, *51*(2), 1–27. doi:10.1145/3172869

Utkin, L. V., Zaborovsky, V. S., & Popov, S. G. (2017). Siamese neural network for intelligent information security control in multi-robot systems. *Automatic Control and Computer Sciences*, *51*(8), 881–887. doi:10.3103/S0146411617080235

Wang, H. (2020). Research on computer network information security and its protection strategy based on secure big data. *IOP Conference Series. Materials Science and Engineering*, *740*(1), 12124. doi:10.1088/1757-899X/740/1/012124

Woo, S., Jo, H. J., Kim, I. S., & Lee, D. H. (2016). A practical security architecture for in-vehicle CAN-FD. *IEEE Transactions on Intelligent Transportation Systems*, *17*(8), 2248–2261. doi:10.1109/TITS.2016.2519464

Zegzhda, D. P. (2016). Sustainability as a criterion for information security in cyber-physical systems. *Automatic Control and Computer Sciences*, *50*(8), 813–819. doi:10.3103/S0146411616080253

Zhang, L. X. Z., Mouritsen, M., & Miller, J. R. (2019). Role of Perceived Value in Acceptance of "Bring Your Own Device" Policy. *Journal of Organizational and End User Computing, 31*(2), 65-82.

ENDNOTES

[1] Zhu Xiaomeng in the School of Public Administration, Hohai University, Nanjing, 211100, China,who is the Corresponding Author, email:442828279@qq.com

[2] Zhu Xiaomeng, School of Public Administration, Hohai University, Nanjing, 211100, China