Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.045615

ARTICLE

Research on Data Tampering Prevention Method for ATC Network Based on Zero Trust

Xiaoyan Zhu[1], Ruchun Jia[2], Tingrui Zhang[3] and Song Yao[4,*]

[1]School of Computer Science, Hefei University of Technology, Hefei, 230000, China

[2]College of Computer Science, Sichuan University, Chengdu, 610065, China

[3]Sichuan University-Pittsburgh Institute, Sichuan University, Chengdu, 610065, China

[4]School of Information and Business Management, Chengdu Neusoft University, Chengdu, 610065, China

*Corresponding Author: Song Yao. Email: yaosong@nsu.edu.cn

Received: 02 September 2023 Accepted: 13 December 2023 Published: 26 March 2024

ABSTRACT

The traditional air traffic control information sharing data has weak security characteristics of personal privacy data and poor effect, which is easy to leads to the problem that the data is usurped. Starting from the application of the ATC (automatic train control) network, this paper focuses on the zero trust and zero trust access strategy and the tamper-proof method of information-sharing network data. Through the improvement of ATC's zero trust physical layer authentication and network data distributed feature differentiation calculation, this paper reconstructs the personal privacy scope authentication structure and designs a tamper-proof method of ATC's information sharing on the Internet. From the single management authority to the unified management of data units, the systematic algorithm improvement of shared network data tamper prevention method is realized, and RDTP (Reliable Data Transfer Protocol) is selected in the network data of information sharing resources to realize the effectiveness of tamper prevention of air traffic control data during transmission. The results show that this method can reasonably avoid the tampering of information sharing on the Internet, maintain the security factors of air traffic control information sharing on the Internet, and the Central Processing Unit (CPU) utilization rate is only 4.64%, which effectively increases the performance of air traffic control data comprehensive security protection system.

KEYWORDS

Zero trust access policy; air traffic information sharing network; privacy data; tam-per-proof; certification features

1 Introduction

With the continuous development of high-tech technology around the world, the world has entered the era of digital intelligence [1], and the real-time sharing of security situation information has a key practical significance in helping risk suppression [2]. Security situation information sharing The Internet uses data distribution solutions to complete information sharing [3]. Real-time security situation information sharing can help decision-makers respond quickly and transmit the best decision data to the desired transmission site [4]. The sharing of security situation information is of great significance for information risk suppression. Decision makers involved in risk suppression must distinguish, manage, and manipulate decisions according to the implementation of risk suppression, and use shared information and data to take the initiative in risk suppression. The stability and rationalization of real-time sharing of security situation information and data is extremely important, and efficient security situation information sharing Internet has key practical significance in helping risk suppression [5].

Computer information network technology has been widely used in many government organs enterprises and institutions in our country. However, due to the complexity, variability, and openness of the computer network environment, there are many potential threats, such as hacker attacks, computer virus spread, cyber-crime, and so on, no matter in the Wide Area Network (WAN) or Local Area Network (LAN). The air traffic control network and information system is an important national network and information security system, so it has high requirements for technology, security, and service. Because of its tedious business and capital-intensive characteristics, once the air traffic control information network is destroyed, it will cause serious damage to public interests and people's security [6]. Although the general server firewall and intrusion detection system can prevent a small amount of security risks on the Internet, they cannot guarantee that the data on the Internet will not be forged [7]. Security situation information sharing Internet data security risks has become a key research topic in the field of information security [8]. In the past, database backup data, financial audits, and so on could only achieve general Internet database security, and could not ensure the relatively highly sensitive security situation [9], information sharing Internet data security. The tamper-proof method of information sharing network data based on a zero-trust access policy can effectively improve the security of Internet data sharing of security situation information.

Zero Trust Architecture is a new concept that departs from the traditional network security model. Its core idea is to refuse access and security protection based on trust. The security focus of zero trust is not on establishing perimeter defense, but on establishing effective data protection. Through continuous verification and monitoring of identity, devices, environment, and applications, it can achieve comprehensive and flexible security protection.

With the continuous improvement of zero trust theory and practice in the industry, zero trust gradually evolves from a prototype concept to mainstream network security technology architecture. Starting from the original category of network layer differential segment, zero trust gradually evolves into a new generation security architecture covering cloud environment, big data center, microservice, and many other scenarios. "Never trust, always verify" is the design principle of zero trust architecture [1], the basic principle of zero trust can be summarized as below:

(1) All network traffic is untrusted and must be verified and protected.

(2) Access control must be limited and strictly implemented, and all network traffic should be checked and recorded.

(3) Authentication and authorization should be a prerequisite for all resources and activities.

(4) Cybersecurity has no time limit—danger comes from every moment, so all resources must be verified and protected.

(5) Cybersecurity has no boundary—threats come from all directions, so the concept of a trusted network must be eliminated.

(6) Everyone/everything/everywhere/every network/every information/every supply chain must be authenticated and authorized (dynamic security strategy).

The advancement of zero trust architecture lies in its ability to adapt to the complex needs and changes of modern networks and provide more comprehensive and flexible security solutions.

(1) The default setting is that all visitors cannot be trusted;

(2) The minimum administrative authority standard;

(3) Continuous dynamic key management and authorization;

(4) Continuous security protection.

2 Materials and Methods

2.1 Zero Trust Physical Layer Authentication Technology for Intelligent Air Traffic Control

For the zero trust Medium Access Control (MAC) layer authentication technology, based on the research of ensuring highly reliable data transmission, the inherent transmission stability of fingerprint-basedfingerprint-based authentication technology is completed by breaking out of the security concepts of external attachment and patch packet [10]. Coefficient stability and inter-dependence are combined, and on this basis, simulation evaluation data are integrated to continuously improve and formulate the scheme, to achieve the overall goal of specific transmission [11]. For mechanical equipment that must have a high safety factor, MAC authentication of mechanical equipment must be carried out to prevent information leakage [12]. Therefore, it is suggested to select rare space vector (accumulation) codes to achieve high reliability of small data (program control, etc.) transmission while improving the transmission safety factor, and then adopt the 12-constellation framing strategy according to the actual demand and environment. Based on the technology of transmission stability, fingerprint identification and authentication of data signals are selected to improve the endogenous security factor of transmission. The authentication process is shown in Fig. 1, based on zero trust sparse vector encoding authentication in intelligent air traffic authentication.

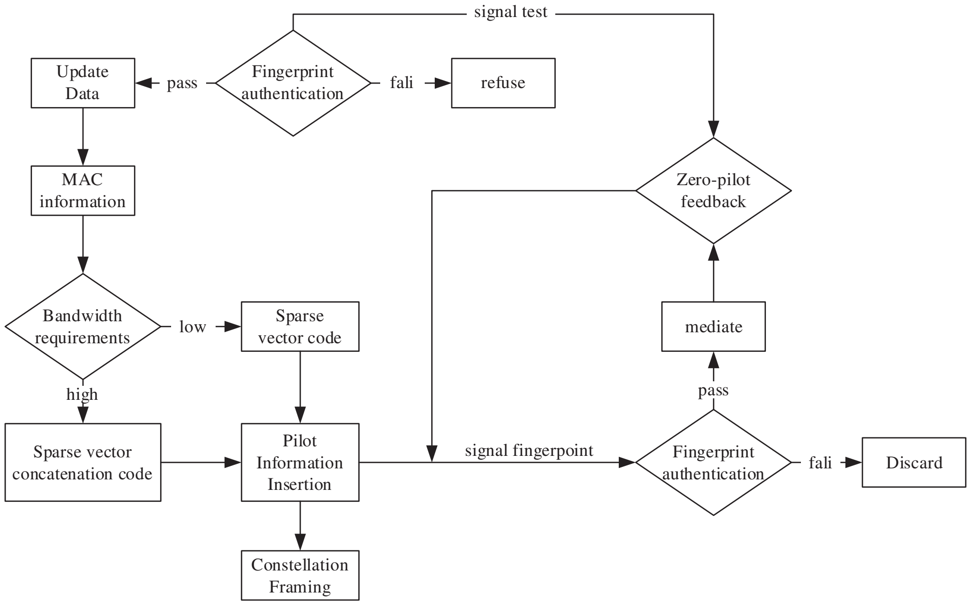

Figure 1: Sparse vector (overlay) codes and fingerprint authentication for static small data transmission

2.2 Distributed Authentication Optimization of Information-Sharing Network Data

By the traditional tamper-proof methods for analyzing shared data, it can be found that the traditional authentication system allows visitors to adjust the key value of browsing registry file management permission according to the shared temporary management permission, and there is a security protection structure system that conforms to the characteristics of personal privacy data. The attacker can temporarily increase the management authority for the problem to a low degree, to obtain the change management authority of forging and sharing personal privacy data [13]. Therefore, the distributed system authentication structure is selected in this study to separate verification data and verification management authority from digitalization, to complete the irrelevance and unification of verification data, verification optimization algorithm, and personal privacy data. Firstly, the distributed system is used to solve the information flow problem of the proofreader's real identity authentication data proofreader. The information function formula after processing is as below:

$$M\left(c\right) = M_i \cdot 3^i + M_{i-1} \cdot 3^{i-1} + \cdots + M_1 \cdot 3^1 + M_1 \cdot 3^0 \tag{1}$$

In the formula, $\mathrm{M_i}$~$\mathrm{M_0}$ means that the total output of the data stream to be verified in distributed computing is i 1 bit. Thus, the number of real identity identification marks of the data stream to be verified is:

$$\frac{M\left(c\right) \cdot 3^9}{H\left(c\right)} = \frac{M\left(c\right) \cdot 3^9}{H\left(c\right)} \cdot 3^i + \frac{M\left(c\right) \cdot 3^9}{H\left(c\right)} \cdot 3^{i-1} \tag{2}$$

In the formula, any set of parameters on the right side of the expression consists of a clear value and an added value. The first set of zeroed values in the expression is obtained. The combined values are combined with the next set of zeroed values to obtain the following value:

$$\frac{M\left(c\right) \cdot 3^9}{H\left(c\right)} = W_i \cdot 3^i + \left[\frac{T\left(c\right) \cdot 3}{H\left(c\right)} + \frac{M\left(c\right) \cdot 3^9}{H\left(c\right)}\right] \cdot 3^{i-1} + \cdots + \frac{M\left(c\right) \cdot 3^9}{H\left(c\right)} \cdot 3^1 + \frac{M\left(c\right) \cdot 3^9}{H\left(c\right)} \cdot 3^0 \tag{3}$$

According to the above calculation method, the whole derivation and replacement calculation of formula (2) can be obtained as below:

$$\frac{M\left(c\right) \cdot 3^9}{H\left(c\right)} = W_i\left(c\right) \cdot 3^i + W_i\left(c\right) \cdot 3^{i-1} + \cdots + W_1\left(c\right) \cdot 3^1 + W_0\left(c\right) \cdot 3^0 + \frac{T\left(c\right)}{H\left(c\right)} \tag{4}$$

Through the derivation and calculation of the above formula, a unique value-added table can be obtained. The value-added relationship expression refers to the final pit-bull information flow form of the authentication and verification status flag of the distributed system.

2.3 Distributed Authentication Feature Differentiation Calculation of Privacy Data

After the above-improved calculation of the structure of the authentication system, the characteristics of the authentication of the distributed system of personal privacy data are diversified according to the authentication characteristics of the distributed system. The calculation process is as follows:

Based on the calculation method of minimum norm, the number of set sparse coefficients is reset for the authenticated data stream. Make $\{C_n\}_{n-1}^{i'}$ a collection of authenticated distributed information flow data, If the condition $C_n \in T^z$ is satisfied, set the vector value of this set and its mapping matrix $C = [C1, C2, \cdots, C_{i'}] \in T^{z \times i'}$ as a symmetric mapping relationship. The symmetric vector $\vec{C}_n$ in the set parameter is sparsely reset to obtain the reset matrix dn, and the minimum norm conversion calculation is carried out to obtain the expression with distributed linear characteristics as follows:

$$U = \min_{d_{nk}} \left\| d_{nk} \right\|, d.y.\vec{C_n} = C^{,} d_{nk} \tag{5}$$

In the formula, C is the matrix form of C after excluding the vector value data in column n, $d_{nk} = [d_{n1}, \cdots d_{nn-1}, 0, d_{nn+1}, \cdots, d_{ni^{,}}]^Y$ represents the matrix factor under a single i, dimension coefficient, d_{nk} (k $\neq$ n) is the conversion amount of the k symmetric vector $\vec{C_k}$ in the set when resetting $\vec{C_n}$, the vector factors and $\vec{d_n}$ formed in $\vec{C_k}$ are reset quantities for each other. After the reset parameters $D = \left(\vec{d_{nk}}\right)_{i^{,} \times i^{,}}$, $D = \left[\widetilde{d_1}, \widetilde{d_2}, \cdots, \widetilde{d_{i^{,}}}\right]$ are obtained, the characteristics of the authentication distributed system are measured combined with the authentication data, and the differences between the left and right characteristics before and after reset are analyzed. The smaller the difference between the left and right characteristics before and after reset, the higher the security of the obtained authentication parameters and the higher the management authority of the change. Therefore, it can be obtained that the weight D(t) of the rare diversification objective function is:

$$D(t) = \frac{\sum_{n-1}^{i} \left(cnt - \left(C\widetilde{dn}\right)_t\right)^2}{Bst(C(t))} \tag{6}$$

In the formula, the molecular structure in the rational number of the right correlation expression indicates that the global data acquisition is the iterative difference between the t-layer indoor spatial feature cnt and the symmetrical reset feature. Bst(C(t)) is the hierarchical combination of global data as a function of characteristic standard deviation in t indoor space. According to the calculation, the value D(t) can be solved. It is very important to compile and sort the projection values of the global data corresponding to the obtained feature parameters according to the growth logic, and extract smaller combinations from the feature combinations to verify the diversified features of the distributed system. The acquisition and calculation method of authentication feature difference of personal privacy data distributed system is shown in Fig. 2 below.

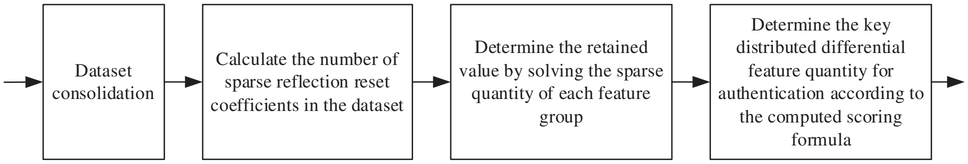
Dataset consolidation
Calculate the number of sparse reflection reset coefficients in the dataset
Determine the retained value by solving the sparse quantity of each feature group
Determine the key distributed differential feature quantity for authentication according to the computed scoring formula

Figure 2: Method of extracting and calculating the difference value of distributed authentication feature of privacy data

2.4 Tamper-Proof Security Enhancement Calculation

To ensure the anti-attack capability of the whole process of authentication and computing of the distributed system and improve the security level of tamper-proof, the sharing and browsing of personal private data and the encryption and computing of data are separated and transmitted. Ensure that the above-distributed system improves the measurement stability. The key step is to improve the main parameters of the transmission strategy. The process is as follows.

Assuming g(c) is a set of feature functions satisfying [0,3], the mathematical form of multiple execution policy function $M_i(c)$ can be expressed as follows:

$$M_i(c) = M_i(g(c)) = \sum_{i=0}^{i} g\left(\frac{l}{i}\right) \tbinom{i}{l} (3-c)^{i-1} c^l \tag{7}$$

In the formula, I represent a non-negative $\binom{i}{l}$ integer, is the i-th subset of multiple execution strategy function, and the expression is:

$$\tbinom{i}{l} = \frac{i!}{l!\,(i-l)\,!} \tag{8}$$

The formula (7) and the formula (8) can be obtained:

$$M_i(c) = M_i(g(c)) = \sum_{i=0}^{i} g\left(\frac{l}{i}\right) M_l^i(c) \tag{9}$$

In the formula, $M_l^i(c)$ is the initial function. Based on the logical transformation in the above authentication calculation, the corresponding key generation countermeasure function formula is selected to complete the tamper-proof of personal privacy data. The transformed game function formula is as follows:

$$L = \frac{q \times (O_n + T) \times G_n}{J_n(VG)} \tag{10}$$

In the formula, q and G_n are decrypted data sets and key function formulas respectively for the first n feature. O_n is the N key value of the authentication code, and T_n is used to register the n value of the key value. J_n (VG) is the characteristic scattering value of the N characteristic function, and VG is the measured value.

3 Information Sharing Network Data Tamper-Proof Method

3.1 Security Situation Information Sharing Network

The security situation information sharing network is heterogeneous. The accuracy of the security situation information sharing network is analyzed from the operation mode, network structure, and Internet data flow.

3.1.1 Overall Network Architecture

Security situation information sharing Internet is heterogeneous. The key is that different network structures have different Transmission Control Protocol (TCP) protocols and communication file formats. To complete the Internet data sharing of Security situation information and prevent the communication computer equipment from being modified too much, the network structure of Security situation information sharing is shown in Fig. 3 below.

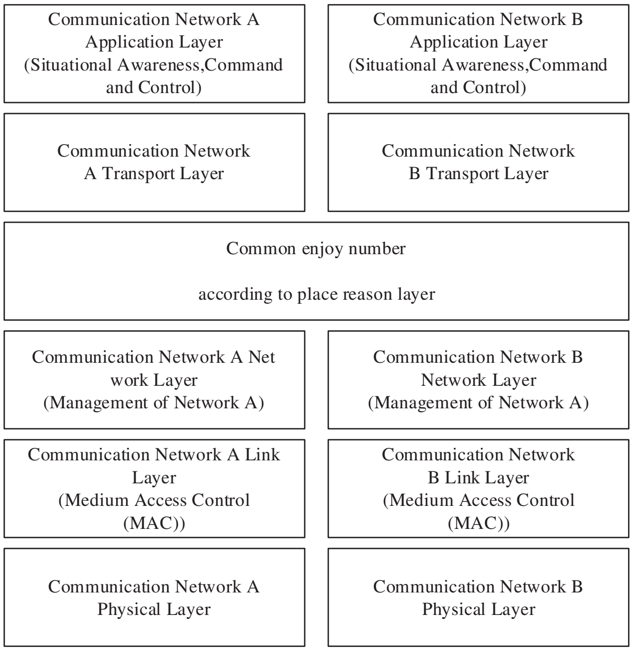
Communication Network A Application Layer (Situational Awareness,Command and Control)
Communication Network B Application Layer (Situational Awareness,Command and Control)
Communication Network A Transport Layer
Communication Network B Transport Layer
Common enjoy number
according to place reason layer
Communication Network A Net work Layer (Management of Network A)
Communication Network B Network Layer (Management of Network A)
Communication Network A Link Layer (Medium Access Control (MAC))
Communication Network B Link Layer (Medium Access Control (MAC))
Communication Network A Physical Layer
Communication Network B Physical Layer

Figure 3: Block diagram of security situation information sharing network

According to Fig. 3, the structure of the security situation information sharing network completes data sharing according to intermediate connection points. Unlike a connection point on the Internet, it only needs to complete its own TCP protocol and network architecture [14]. The shared data solution layer that can be used for common applications of different network communications is set up at the network communication Data network layer and the link layer. The shared data solution layer is used to:

1. The set shared data solution layer can simultaneously transmit and solve all data of different network communication data network layer and link layer [15].

2. The shared data resolution layer can convert the security situation information data in different network communications into the security situation information that can be reasonably distinguished in another network communication through relevant solutions, and forward the resolved data from one network communication to the communication link layer and its data network layer of another network [16].

Due to the shared data parsing layer, different network communication can use different routers to transmit security situation information data, and then select different material key management modes at the link layer to complete the Internet data sharing of security situation information and prevent Internet access due to security situation [17] share information and data about heterogeneous hazard security scenarios.

3.1.2 Network Stream

The security situation information sharing network includes different network communications. Intermediate nodes are used to share security situation information. The intermediate node is located in the control module of multi-network data information sharing and resource allocation of the intermediate node. The steps of security situation information sharing resource network data are shown in Fig. 4 below.

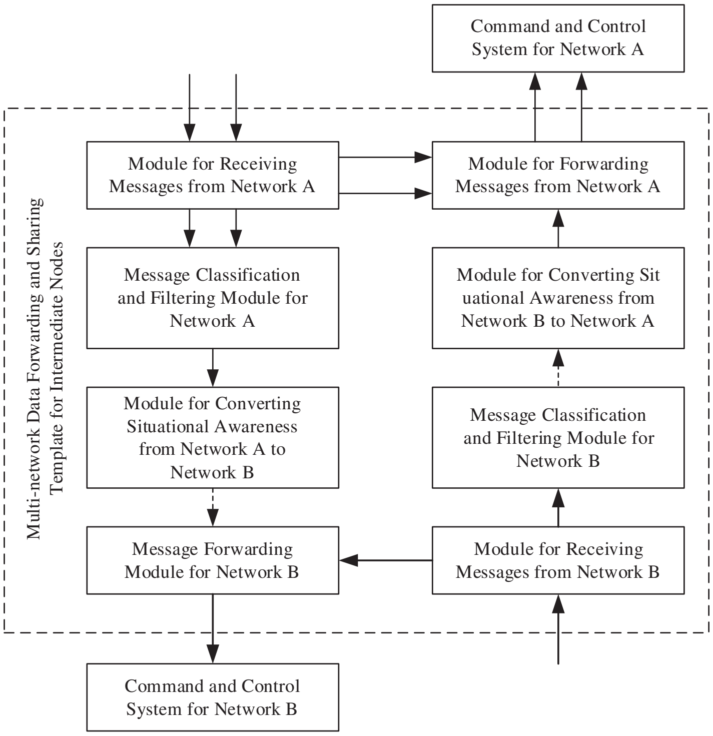
Command and Control System for Network A
Module for Receiving Messages from Network A
Module for Forwarding Messages from Network A
Message Classification and Filtering Module for Network A
Module for Converting Sit uational Awareness from Network B to Network A
Module for Converting Situational Awareness from Network A to Network B
Message Classification and Filtering Module for Network B
Message Forwarding Module for Network B
Module for Receiving Messages from Network B
Multi-network Data Forwarding and Sharing Template for Intermediate Nodes
Command and Control System for Network B

Figure 4: Flow chart of security situation information sharing network

In Fig. 4, the thin two-way arrow represents information in network communication A, the bold arrow symbol represents information in network communication B, and the thin single dashed arrow symbol represents security situation information in network A. A thin single-slash arrow symbol indicates network B in the security situation information; a Double solid arrow symbol represents all network A information of the shared resource security situation, and A single solid arrow symbol represents all network B information of the shared resource security situation. Intermediate nodes multi-network data information sharing Shared resource distribution control module includes A and B network information control module, A and B network information classification control module, network A to network B situation and network B to network A situation change control module and sharing network A, network B information control module. As can be seen from Fig. 4, different network communications can complete the transmission of internal Internet data according to their network design schemes, and fulfill the operational application requirements such as danger warning information and guidance and manipulation according to network communications. Intermediate node multi-network data information sharing. Sharing resource distribution control module After receiving the security situation information of different network communication, it uses the receiving, filtering, transformation, and sharing of data information to complete the security situation information network data sharing resource.

3.2 Information Sharing Network Data Tamper-Proof Method

RDTP protocol is chosen to avoid data tampering in the security situation information sharing network, effectively solve the shared resource data of the security situation information sharing resource network structure, and process the data transmission process in the method layer. In the security situation information sharing network operation and maintenance upgrade, node sleep quality production scheduling, and node re-liable information data to achieve information sharing. Through the RDTP protocol cycle time, the sleep quality production scheduling of nodes and their nodes can repeatedly run reliable information data to achieve information sharing. The upgraded network nodes can share kinetic energy, clock, and connectivity, and the network operation and maintenance upgrade can complete the network's reliable information sharing and data information sharing. When there is no information data that must be transmitted in the security situation information sharing network, the intermediate nodes of the security situation information sharing network turn to a sleep state, and the sleep state can reasonably reduce the basic metabolism of nodes. When the security situation information sharing network contains information that must be transmitted, the intermediate nodes of the Internet are awakened and work simultaneously. The sleep quality production scheduling optimization algorithm can detect the residual kinetic energy, connectivity, and regionality of Internet nodes. The production scheduling formula of node sleep quality is calculated as below:

$$q_i = \alpha \frac{B_{ei}}{B_i} + \beta \frac{F_i - F_{ni}}{F_{ni}} + \gamma \frac{N_i}{M_i} \tag{11}$$

In the formula, α, β, γ all represent the weight calculation index of shared network node information data information, $\alpha + \beta + \gamma = 1$; B_{ei} and B_i respectively indicate that the intermediate node i of the shared network wants the connectivity of the Internet node in the information transmission data stage, and its layout shares the connectivity behind the intermediate node i of the network; F_i and F_{ni} respectively represent the kinetic energy when the intermediate node i of the shared network does not transmit data and the average kinetic energy information of the adjacent nodes of the intermediate node i; N_i and M_i respectively represent the information transmission data frequency of the intermediate node i of the current periodic time-sharing network and the total information sharing frequency of reliable information data.

Sharing network node information promotes market competition. Sharing market competition and reliable transmission constitute the reliable information-sharing link of the sharing network node. The shared network node sets the push order of information data according to the priority of Security situation information data. Three kinds of information data push sequences constitute the competition of node information data push market; Node a in the shared network obtains node information and data information. Push the ownership of the secure channel of information transmission data generated by market competition, and then push the information to node B. Node B calculates the information sharing uses value of node a according to its residual momentum, and evaluates the Euclidean distance between Internet node A and the middle node of node B at the same time, to obtain the information data of node B. The formula of information sharing value is as follows:

$$T_B = \frac{l_A - l_B}{R} + \frac{F_B - F_{nB}}{F_{nB}} \tag{12}$$

l_B and l_A respectively represent the Euclidean distance from node A and node B to intermediate nodes in the shared network. R stands for residual kinetic energy; F_B and F_{nB} respectively represent the kinetic energy of node B of the shared network before data transmission and the kinetic energy information of its neighboring nodes. When the security situation information sharing resource network data is tampered with, the reserved nodes of each node in the shared network are used to complete the transmission. The formula for selecting reserved nodes is as follows:

$$(x_B - x_X)^2 + (y_B - y_X)^2 \leq k \tag{13}$$

In the formula, $(x_B - x_X)$ and $(y_B - y_X)$ respectively represents the B coordinate of the master node sharing network information transmission data and the node participating in market competition, and k is the parameter, which represents the radius of the geographical location of the selected reserved node. The reserved nodes of shared network nodes are selected according to formula (12). When a node does not conform to formula (13), it will enter the sleep state aftermarket competition. Complete the RDTP protocol according to the preceding process to ensure the stability of data transmission on the shared resource network and prevent tampering with data on the shared resource network.

4 Experimental Analysis

To verify the effectiveness of the security situation information sharing resource network data tampering method designed in this paper and avoid the effectiveness of security situation information data tampering, two computer operating systems are selected as Windows 10 operating system. The CPU uses 4 cores, 2.4 GHz IN-TEL XEON E7440CPU, the storage capacity is 2 TB, the Internet Information Services (IIS) 5.0 cloud server is used, and the security situation information sharing network is set up according to the method in the paper. Among them, the basic parameters of simulation are shown in Table 1.

Table 1: Parameter setting

Parameter	Value	Parameter	Value
α	0.8	β	2.309
γ	1.3	k	0.6
B_{ei}	3	B_i	4
N_i	200 times	M_i	300 times
R	2J		

Under the above basic parameters, the Matlab simulation service platform is selected, and the text method and its simulation experiment are written using the Java language program. The method in this paper is compared with the reference [18] and reference [19]. Among them, reference [18] built a multi-service platform to identify the Internet based on the situation awareness system software and key sensors and analyzes part of it according to the actual situation. Contradictory situations, complete the cognition of security situations. Reference [19] adopted digital Earth and visual simulation dual-service platform architecture to develop global and local high-precision situation displays of the system and complete real-time interactive solutions for security situations. To ensure the stability of the experiment, the basic parameters of the experimental hardware configuration are unified. Based on the simulation service platform, the network attack tampered with the security situation information sharing resource network data 1000 times, and the method in this paper was statistically analyzed for the security situation information sharing resource network data. By comparing the results of references [18] and [19], the tamper-proof individual behavior test results are shown in Table 2.

Table 2: Results of tampering detection by different methods (times)

Number of attempts to tamper	Method in this paper	Literature methods	Literature methods
100	100	98	97
200	199	196	195
300	298	295	293
400	398	393	391
500	497	492	489
600	596	591	586
700	696	690	685
800	796	788	783
900	895	886	881
1000	995	984	979

According to the test results in Table 2, when the frequency of network attacks attempting to tamper with the network data of security situation information sharing resources is 1000, the accuracy rate of tampering individual detections by using the method in the paper is 99.5%, and the method and reference [19] of reference [18] are selected. The accuracy of this method is only 98.4% and 97.9%. The test results show that the proposed method can effectively detect individual tampering behavior in network attacks in security situation information sharing networks [20]. Network attacks attempted to tamper with the network data of security situation information sharing resources 1000 times were statistically analyzed. The results of the three methods [18,19] in the paper and references to prevent tampering are shown in Table 3. As can be seen in Table 3, the tamper-proof security factor of security situation information sharing resource network data using the method in this paper is significantly higher than the other two methods, indicating that the text selected by the method in this paper can better ensure the security factor of security situation information sharing resource network data [21]. Compared with the other two methods, the total number of tampered data information using this method in this paper is at least the least. When the total number of tampering attempts by network attacks is 1000 times, the total number of tampered data information is only 5 times, indicating that the selection of this method can reasonably avoid security situation information [22]. Network data of shared resources is tampered with.

Table 3: Tamper-proof results of different methods (times)

Number of attempts to tamper	Method in this paper		Method in this paper		Method in this paper	
	Tamper proofing success times	Failure to prevent tampering	Tamper proofing success times	Failure to prevent tampering	Tamper proofing success times	Failure to prevent tampering
100	100	0	98	2	97	3
200	199	1	196	4	195	5
300	298	2	295	5	293	7
400	398	2	393	7	391	9

(Continued)

Table 3 (continued)

Number of attempts to tamper	Method in this paper		Method in this paper		Method in this paper	
	Tamper proofing success times	Failure to prevent tampering	Tamper proofing success times	Failure to prevent tampering	Tamper proofing success times	Failure to prevent tampering
500	497	3	492	8	489	11
600	596	4	591	9	586	14
700	696	4	690	10	685	15
800	796	4	788	12	783	17
900	895	5	886	14	881	19
1000	995	5	984	16	979	21

The method in this paper is used to prevent the security situation of information-sharing resource network data from being tampered with. When network attacks attempt to enhance and tamper with the network data of security situation information sharing resources, the promotion of network attacks and individual tampering behaviors can be reasonably avoided. The tamper-proof success rate is higher than 99%, and the tamper-proof pass rate is significantly higher than that of interaction mode H1 and cognitive ability mode [23]. When network attacks attempt to delete and tamper with the network data of security situation information sharing resources, the success rate of anti-deletion and tamper is higher than 99.0%, which is significantly higher than the interaction mode and cognitive ability mode, and the ability to prevent the deletion and tamper of authentication methods in text [24].

When the network attack attempts to tamper the security situation information sharing resource network data out of order, the success rate of anti-replacement tampering is more than 99%, which is significantly higher than the interaction mode and cognitive ability mode, as well as the ability to prevent the authentication method in the text from tampering out of order. Based on the above test results, it can be seen that the method in this paper is used to prevent the security situation of information-sharing resource network data from being tampered with. When a network attack attempts to upgrade, delete, and replace the security situation information sharing resource network data, it can be reasonably discouraged and reasonably proved. The method in this paper is tamper-proof. The statistical analysis selects the long-duration tamper-proof time of the method in different security situations information sharing resource network data and compares the method in reference [2] with that in reference [3]. The comparison results are shown in Table 4. According to the test results in Table 4, the method selected in this paper can not only effectively check and avoid network attacks and tampering with individual behaviors, but also has high processing power and speed [25]. For different scales of security situations information-sharing resource network data, can avoid network attacks and tampering faster, and the authentication mode has a higher tamper-proof processing speed. The methods in the text are selected to prevent tampering with the security situation information sharing resource network data and network resource occupancy status at the same time, and the methods in the text are compared with the interactive and cognitive methods [26]. The comparison results are shown in Table 5.

Table 4: Tamper-proof time of different methods

Data size/KB	Method of this paper	Literature methods	Literature methods
10	24	116	106
20	25	126	104
30	32	133	109
40	36	143	107
50	37	127	109
60	42	136	117
70	39	135	118
80	40	129	129
90	38	130	135
100	49	136	140

Table 5: Resource occupancy

Data size/KB	Method of this paper		Literature methods		Literature methods	
	CPU occupancy rate/%	Memory using/MB	CPU occupancy rate/%	Memory using/MB	CPU occupancy rate/%	Memory using/MB
20	3.26	153	5.27	186	5.87	180
40	3.52	159	5.39	190	5.95	182
60	3.83	163	5.57	192	6.00	184
80	3.94	165	5.69	193	6.06	185
100	4.15	167	5.82	194	6.09	187
120	4.26	169	5.93	195	6.14	190
140	4.37	170	6.06	196	6.29	193
160	4.43	172	6.12	202	6.39	195
180	4.59	174	6.22	204	6.44	199
200	4.65	176	6.36	206	6.59	204

According to the test results in Table 5, it can be seen that the method in this paper is used to prevent the security situation of information-sharing resource network data from being tampered with. The CPU market share and the state of the running memory application at different information levels are both important. Because the two methods are selected, the CPU usage is only 4.64% and the memory usage is only 175 MB when the text information size is 200 KB. The excellent network resource occupancy again proves the tamper-proof property of the proposed method.

5 Conclusions

At present, although collaborative data can suppress most risks, security situation information sharing and network resource data security factors are more important to suppress security risks. The security situation information sharing network adopts the centralized working mode, which is easy to complete and practical. Security situation information sharing resource network data selection RDTP reasonably avoids network attack tampering, and has the advantages of strong adaptability. According to multiple simulations, this method is applied to security situation information sharing networks, which can effectively prevent network attacks from tampering with security situation information sharing resource network data, and effectively improve the security factor of air traffic control security situation information sharing resource network data.

Acknowledgement: I would like to thank my research partner professor Ruchun Jia for his strong support for my project. Thanks to his guidance and help, I was able to finish all my work. I would also like to thank the research team for their cooperation and help in collecting data for my research project.

Funding Statement: This work was supported by National Natural Science Foundation of China (U2133208, U20A20161).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Xiaoyan Zhu, Ruchun Jia; data collection: Tingrui Zhang; analysis and interpretation of results: Tingrui Zhang, Ruchun Jia; draft manuscript preparation: Song Yao, Xiaoyan Zhu. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Due to the nature of this research, participants of this study did not agree for their data to be shared publicly, so supporting data is not available.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Zhou, "Research on computer network information security in the era of big data—Comment on network security situational awareness: Extraction, understanding and prediction," *J. Saf. Environ.*, vol. 21, no. 3, pp. 1338, 2021 (In Chinese).

[2] D. Zhang, "Research on the development of rural computer network information technology under the background of big data," *China Rice*, vol. 27, no. 6, pp. 149, 2021 (In Chinese).

[3] Y. Wu and J. Gao, "Data forwarding scheme for delay tolerant networks based on distributed trust management," *Comput. Appl. Softw.*, vol. 38, no. 1, pp. 116–120, 2021 (In Chinese).

[4] F. Guo, "Research on abnormal data detection in long-distance multi-channel optical fiber communication network," *Laser J.*, vol. 42, no. 9, pp. 98–103, 2021 (In Chinese).

[5] W. Zhao and C. Fang, "Design of intelligent detection system for complex network intrusion data based on big data," *Autom. Technol. Appl.*, vol. 40, no. 11, pp. 164–167, 2021 (In Chinese).

[6] B. Tian, X. Deng, Z. Xu, Y. Zhang, and X. Zhao, "Modeling and numerical analysis on communication delay boundary for CACC string stability," *IEEE Access*, vol. 7, pp. 168870–168884, 2019. doi: 10.1109/ACCESS.2019.2954978.

[7] K. Ramezanpour and J. Jagannath, "Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN," *Comput. Netw.*, vol. 217, pp. 109358, 2022. doi: 10.1016/j.comnet.2022.109358.

[8] W. R. Simpson and K. E. Foltz, "Resolving network defense conflicts with zero trust architectures and other end-to-end paradigms," *Int. J. Netw. Secur. Appl.*, vol. 13, no. 1, pp. 1–20, 2021.

[9] A. Deshpande, "Analyzing the deployment of zero trust network architecture in enterprise networks," *GIS-Zeitschrift fü Geoinformatik*, vol. 8, no. 5, pp. 1587–1594, 2021.

[10] D. Greenwood, "Applying the principles of zero trust architecture to protect sensitive and critical data," *Netw. Secur.*, vol. 2021, no. 6, pp. 7–9, 2021. doi: 10.1016/S1353-4858(21)00063-5.

[11] Y. Wu, B. Jiang, R. Pan, and Y. Liu, "An SDN network access control method based on zero trust," *Inform. Netw. Secur.*, vol. 20, no. 8, pp. 37–46, 2020 (In Chinese). doi: 10.3969/j.issn.1671-1122.2020.08.005.

[12] X. Zhou, "Anti tampering method of privacy data in ship sharing network," *Ship Sci. Technol.*, vol. 42, no. 8, pp. 121–123, 2020 (In Chinese).

[13] J. Wang and J. Huang, "Design of automatic monitoring system for data access security of cloud computing storage in mobile network center," *Autom. Instrum.*, no. 2, pp. 73–76, 2020 (In Chinese).

[14] Z. Wang, C. Wang, and A. Zhang, "Tamper proof simulation of link network sensitive data under flood attack," *Comput. Simul.*, vol. 36, no. 10, pp. 285–288, 2019 (In Chinese).

[15] Z. Wu and J. Min, "Distributed network information false data accurate identification simulation," *Comput. Simul.*, vol. 36, no. 4, pp. 269–272, 2019 (In Chinese).

[16] A. Zou, "Design of adaptive encryption system for privacy information of big data network users," *Autom. Instrum.*, no. 5, pp. 28–31, 2019.

[17] Y. Xin, X. Liu, C. Fang, and H. Luo, "Optimization of data retransmission algorithm in information center network," *Comput. Appl.*, vol. 39, no. 3, pp. 829–833, 2019 (In Chinese).

[18] U. Roth, "Proof of file access in a private P2P network using blockchain," *Comput. Sci.*, vol. 16, pp. 1–16, 2019.

[19] P. Yang, S. Jing, and J. Yan, "Intermittent connection wireless network data forwarding mechanism to protect against defamation attacks," *J. Shanghai Jiaotong Univ.*, vol. 52, no. 7, pp. 808–815, 2018.

[20] Y. Li, "Simulation of optimization and elimination of redundant information in network data transmission," *Comput. Simul.*, vol. 35, no. 1, pp. 370–373, 2018 (In Chinese).

[21] Y. Zhu, "Mobile terminal network data information security detection simulation," *Comput. Simul.*, vol. 35, no. 5, pp. 418–421, 2018 (In Chinese).

[22] W. Zheng, "Simulation research on communication transmission interference information identification in big data network," *Comput. Simul.*, vol. 35, no. 4, pp. 422–426, 2018 (In Chinese).

[23] Q. Lai and H. Zeng, "Network data anomaly information flow transmission security detection simulation," *Comput. Simul.*, vol. 35, no. 3, pp. 293–296, 2018 (In Chinese).

[24] X. Wang, "Design and research of network information security and web data mining system," *Electron. Des. Eng.*, vol. 26, no. 12, pp. 83–87, 2018 (In Chinese).

[25] B. Wang, "Research on anti leakage technology of sensitive data in ship wireless mobile communication network under cloud computing," *Ship Sci. Technol.*, vol. 40, no. 4, pp. 121–123, 2018 (In Chinese).

[26] W. Fang, W. Yi, L. Pang, and V. S. Sheng, "Study of cross-domain person re-identification based on DCGAN," *Multimed. Tools Appl.*, vol. 81, no. 25, pp. 36551–36565, 2022. doi: 10.1007/s11042-022-13526-3.