electronics

MDPI

Article

Research on Invulnerability Technology of Node Attack in Space-Based Information Network Based on Complex Network

Chengxiang Liu [1], Wei Xiong [2,*], Ying Zhang [1], Yang Sun [2], Minghui Xiong [1] and Chao Guo [1]

[1] Graduate School, Space Engineering University, Beijing 101416, China; 201311141033@mail.bnu.edu.cn (C.L.); yinggarfield1986@sina.com.cn (Y.Z.); xtkxxmh@163.com (M.X.); gch_87_10_26@126.com (C.G.)

[2] Science and Technology on Complex Electronic System Simulation Laboratory, Space Engineering University, Beijing 101416, China; fireflypd@buaa.edu.cn

* Correspondence: 13331094335@163.com; Tel.: +86-185-1861-9059

Received: 19 March 2019; Accepted: 30 April 2019; Published: 8 May 2019

Abstract: With the rapid development of communications technology, the space-based information network (SBIN) is increasingly threatened by the outside world. Dynamic changes in any part of its interior can cause the collapse of the entire network. Therefore, research on the invulnerability of SBIN has become an urgent need to promote the economic development of our country and improve the living standards of our people. To this end, this paper has carried out research on the node-attacked invulnerability of SBIN based on the complex network theory. First, based on the model of SBIN, the internal parameters of the network are analyzed theoretically based on complex networks. Second, the paper proposes an improved tree attack strategy to analyze the invulnerability of SBIN, which constitutes a problem where the traditional attack strategy has a low invulnerability and the connected edge cannot fully realize the network function. Then, based on the improved tree attack strategy algorithm, this paper optimizes the invulnerability of SBIN by constructing four different edge-increasing strategies. Through the research, the LDF edge-increasing strategy makes the entire network flatter and can effectively improve the network's ability to resist destruction. The research of invulnerability based on the complex network has a certain technical support and theoretical guidance for the construction of a reasonable and stable SBIN.

Keywords: space-based information network (SBIN); node attack; invulnerability; complex network

1. Introduction

With the full improvement of the function of SBIN, its task units are increasing. This makes the information interaction among subsystems become intricate and complex, and the relations among subsystems develop rapidly towards the direction of network, interconnection and intercommunication. In the process of executing tasks, all kinds of nodes of SBIN are always faced with random interference from space targets and deliberate attacks by the enemy, which reduces the invulnerability of SBIN greatly [1]. Under such a background, the dynamical change of any components could trigger a chain reaction, and even bring down the entire network. Therefore, the analysis of the invulnerability of SBIN is an important indicator to evaluate its effectiveness and security. Invulnerability is an important indicator used to describe the damage degree of a communication service under the premise of network failures [2]. These failures can include all kinds, such as communication software errors, network performance degradation due to traffic congestion, the breaking of a communication cable or a communication equipment fault, and so on [3–8].

For the sake of a comprehensive reflection of the invulnerable degree of SBIN, it is necessary to carry out research on the invulnerability. The adoption of a rational model and simulation analysis

technique, through which the weakness of SBIN can be found out, lays the solid foundation of a design to reinforce the weakness in order to build up an excellent platform that can satisfy future battlefield environment requirements.

2. Related Works

As a significant research method on complex giant systems, the complex network theory highlights the topological characteristics of the system structure, which is an important basis to describe the whole network node abstraction and connection relation. Nowadays, the complex network theory has been widely used in the network characteristic analysis, structure optimization, vulnerability and invulnerability analysis of the Internet, traffic network, power network, communication network and optional network, which results in a series of achievements [9–16].

At present, the network failure caused by node attacks is a hot topic in research. Ding et al. [17] proposed a location-based a similarity detection scheme using deployment knowledge in wireless sensor networks to solve network attacks that generate replication nodes due to being unattended; In addition to focusing on the physical connection topology of SBIN, the study on the invulnerability of SBIN also needs to focus on the other network attributes, such as the degree distribution, betweenness, clustering coefficient, and so on [18–20]. It is of great value to grasp these characteristics and rules. In particular, the hidden dangers in software or application programs put forward higher requirements and challenges for the information transmission of the whole network, and it is the key issue of current research to adopt different defense measures to realize vulnerability mining. When reading a lot of literature, this paper found that, in [21], different defense measures were explained in detail to evaluate the vulnerability in a web application, which can be used to identify the most challenging vulnerabilities in the field of web application. Zero-day is also a kind of vulnerability, which can pose a critical threat to the software or application. However, zero-day is difficult to detect through conventional signature-based defenses [22]. In [23,24], a framework was proposed to discover zero-day attacks and estimate the severity of an identified zero-day vulnerability. In [25,26], the frequencies of different vulnerabilities are measured to estimate the security risk-level, which can be used for an automated and reasonable security management, based on the standard CVSS Risk Level Estimation Model. The Quantitative Information Security Risk Assessment Model [27] was designed to enhance the security level of a large open campus network, with a reliable and repeatable risk analysis in a realistic and affordable manner.

Furthermore, the main research methods of the invulnerability of SBIN consist of two parts: the selection of a measure index and the generation of an attack mode [28,29]. In the traditional method, the invulnerability of the network under different topologies is analyzed by deducing and analyzing the measure indexes. This method often ignores the physical connection characteristics of the whole network, making the results of the theoretical analysis meaningless for the actual network evolution. Therefore, based on the improved tree attack strategy, this paper will analyze the invulnerability technology of SBIN.

After analyzing the influence of different attack strategies on the invulnerability of SBIN, this paper further studies the optimization of invulnerability. Based on the related literature, we found that Tian [30] proposed a complex network destructiveness simulation optimization algorithm based on a TABU search, to continuously optimize the target function with natural connectivity as the parameter, so as to improve the network invulnerability. The security issues in space information networks have been well surveyed [31,32], from the perspectives of secure handoff, secure transmission control, key management, and secure routing, and a space network security mechanism was proposed to deal with the above security threats. Aiming at a cooperative transmission for space-based networks, many scholars have gone deep into the research of the network architecture, protocols, and routing strategy and routing algorithm. Based on the SOS structure and some other protocols, networking technologies and coordination mechanisms were fully researched to improve the cooperative transmission for Earth observation [33]. Additionally, in [34], a kind of multiple access communication systems, with a GEO

and a LEO satellite as relays, was designed, based on the resource allocation protocol. Wang [35] improves the dynamic intrusion of complex networks by optimizing the load priority prevention strategy index. Chen [36] proposes a new nondestructive measurement index, which is used as the object function of the optimized and improved particle swarm algorithm to ensure the smooth operation of railway transportation. Four typical capability allocation strategies are proposed by Li [37] to improve the dynamic resistance of complex networks and effectively prevent cascading failures of complex networks under limited resources. Based on a large amount of relevant research, this paper conducts an in-depth study on the problem of invulnerability optimization of SBIN.

3. Model Construction and Parameter Analysis of Space-Based Information Network

SBIN is an integrated space-based and ground-based information network with a certain ability for independent operation management and network reconstruction. It includes spacecrafts with various types of payloads and corresponding operational control systems and application systems. According to the principle of maximum comprehensive utilization of information resources, it takes the spacecraft platform as the hub and adopts the centralized and distributed methods. Through connectivity and information exchange, SBIN makes information acquisition, processing, promotion, transmission and distribution uninterrupted, real-time, safe and reliable. Its functions include navigation, positioning and information transmission, etc., which can be connected with land-based, sea-based and space-based multi-element information systems.

3.1. Construction of Space-Based Information Network Model

Nowadays, SBIN has become an important means for economic countries and military powers to obtain and transmit useful information. It has greatly improved the ability of information sharing and joint command and control, and accelerated the transformation from an information advantage to a decision-making advantage. It can give full play to the subjective initiative of the integration of space and earth, and comprehensively enhance the coordinated development of countries and organizations. SBIN is a network that uses spatial advantages to obtain various kinds of information. It is mainly composed of a GEO backbone network, MEO functional architecture network, and LEO satellite networking and ground terminal access unit. The composition of the SBIN system is shown in Figure 1.

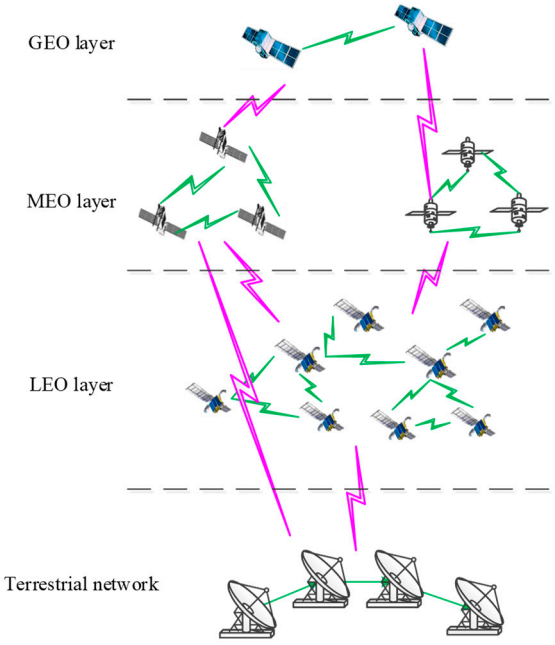

Figure 1. Composition of the space-based information network system.

As can be seen from the composition of the whole SBIN, its internal units are numerous and their connections are intricate. SBIN is mainly composed of four layers, namely the Resource Layer, Service Layer, Function Layer and Mission Layer. The resource layer is mainly composed of GEO, MEO, LEO, and ground connection terminal units and their connection relations. It is the basis from which SBIN performs tasks. Different service businesses can be realized by encapsulating different components. The service layer mainly carries out a series of service functions, such as visible imaging observation, microwave communication and mapping data processing. It is the basis from which SBIN realizes its functions. Through different business services, they are aggregated into the functional layer of SBIN. The function layer has the ability to organize different business services in the service layer so as to achieve a certain kind of function. It mainly includes the data transmission and distribution, environmental information detection, and the position and navigation of a series of modules. The top layer of the function module of SBIN is the mission layer. With the support of different functional attributes in the function layer, SBIN can perform related tasks conveniently and quickly. The functional-relationship diagram of SBIN is shown in Figure 2.

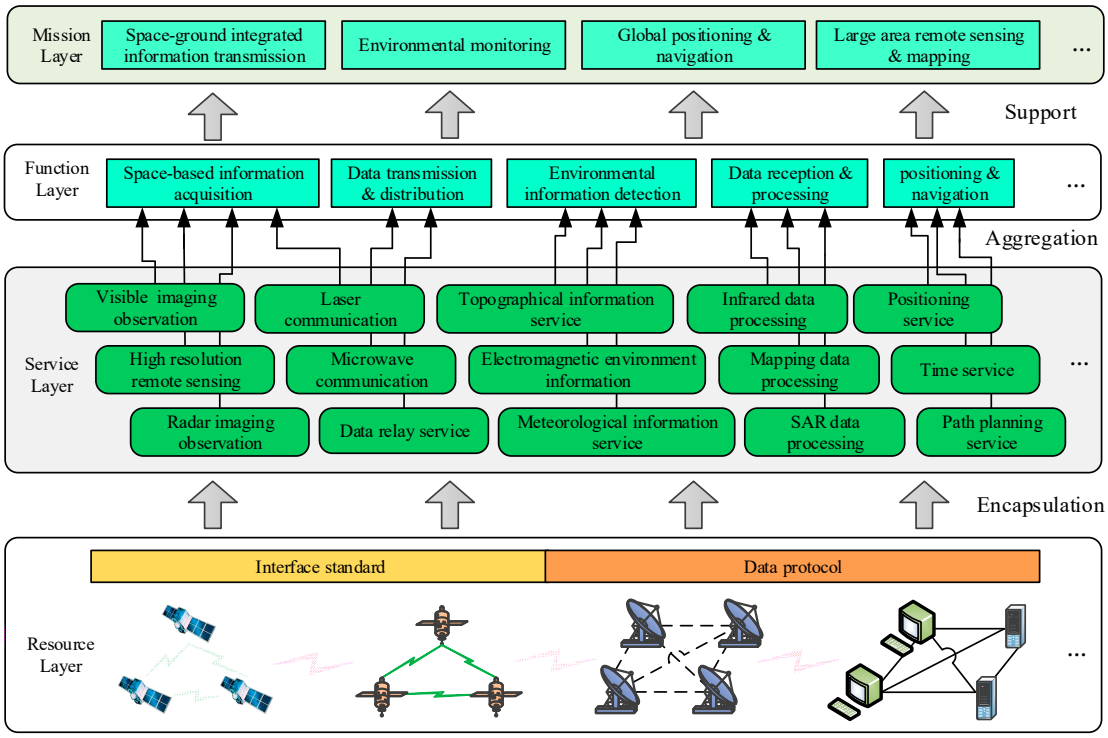

Figure 2. Functional-relationship diagram of the space-based information network.

3.2. Model Mapping Based on Complex Network

3.2.1. Characteristics Analysis of SBIN

With numerous nodes and complex connection relationships in SBIN, the complex network theory provides tools for the interaction and influence of nodes and their connection relationships. Complex-network theory defines the multi-layer, multi-stage, multi-attribute and multi-objective networks nested in SBIN that make the abstract network more concrete to achieve the purpose of facilitating the theoretical analysis and research. Through the complex network theory, the features of SBIN can be summarized in Table 1.

Table 1. Characteristics analysis of the space-based information network.

Complex-Network Characteristics	SBIN Features
Multi-layer features	Information transmission process involves the resource layer, service layer, function layer and mission layer
Multi-stage characteristics	Mainly composed of the bottom distribution sensor, convergence network and terminal application
Multi-dimensional traffic	Transmitted information includes data, images, voice, and video
Multiple attributes/guidelines	Different attributes and guidelines for abstract entities and interactions
Congestion	Network communication capabilities and user information transmission requirements lead to data transmission congestion control problems
Coordinating optimization issues	Global optimization results of data applications under limited resources may not satisfy the optimal data service requirements of individual nodes

3.2.2. Parameter Analysis of SBIN

1. Relationship between nodes and joint edges in the space-based information network

Based on the abstraction of the nodes and connected edges of the SBIN, we established a complex network model $G = \langle V, E \rangle$ to describe the mapping relationship between its nodes and the connected edges, and $V = \{v_i | i = 1, 2, \cdots n\}$, $E = \left\{ e_{ij} \middle| e_{ij} = (v_i, v_j), v_i, v_j \in V \right\}$. $\forall e_{ij} \in E$, there exists a pair of nodes (v_i, v_j) to it, and when there is a connection relationship between the two nodes, $e_{ij} = (v_i, v_j) = 1$, otherwise $e_{ij} = 0$.

This paper introduces the adjacency matrix A to describe the mapping result between nodes and connected edges, which can be expressed as:

$$A = \begin{bmatrix} e_{11} & e_{12} & e_{13} & \cdots & e_{1n} \\ e_{21} & e_{22} & e_{23} & \cdots & e_{2n} \\ e_{31} & e_{32} & e_{33} & \cdots & e_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ e_{n1} & e_{n2} & e_{n3} & \cdots & e_{nn} \end{bmatrix} \tag{1}$$

2. Parameter Analysis of Space-based Information Network Based on Metric Index Parameters

The space-based information network studied in this paper consists of 107 nodes and 324 connected edges, including 5 GEO satellites, 2 HEO satellites, 20 MEO satellites, 35 LEO satellites, 15 space vehicles and 30 ground accesses terminal, and the network topology is shown in Figure 3.

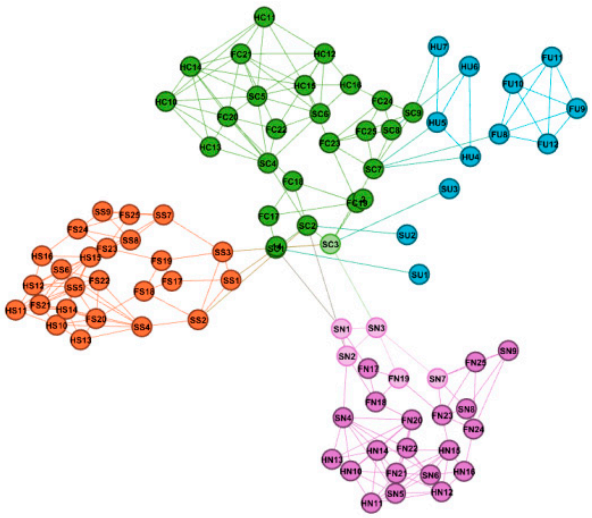

Figure 3. Space topology diagram of the space-based information network.

According to the node composition of SBIN, we statistically calculated the nodes and joint edges participating in the space task. The average degree, average clustering coefficient, average path length and network diameter are calculated to reveal the basic properties of the topology model of SBIN. The parameter analysis of SBIN is shown in Table 2.

Table 2. Parameter analysis of the space-based information network.

Parameter Index	Node Number n	Edge Number m	Average Degree k	Average Clustering Coefficient C	Average Path Length L	Network Diameter D
Data Analysis	107	324	3.028	0.502	2.829	3

4. Algorithm Design of Improved Tree Attack Strategy

After clarifying the topological relationship and parameters index of SBIN, the paper analyzes the invulnerability of the entire network by attacking its internal network structure. From the perspective of the type of attacked object, each of the nodes and edges in the network may become the targets of attack. The attacked target may include the node only, the edge only or the node and edge simultaneously. The study in this paper focus on a SBIN invulnerability analysis based on node attacks. We constructed the attack information model, after which an improved tree-attack strategy is proposed to compare and analyze the invulnerability change of SBIN under the traditional attack strategy. The simulation comparison experiment is operated to verify the effectiveness of the two methods. To establish the invulnerability model of SBIN, the first problem to be solved is the methods and meaning of the attacking node.

4.1. Methods and Meaning of Attacking Node

There are many ways to destroy network nodes. When analyzing the different security threats of vehicular networks, Alberto Petrillo et al. first describe the considered attacks, and then consider these attacks in the experimental evaluation and effects [38–41]. They propose a novel collaborative control strategy for enhancing the protection level of autonomous platoons. A detailed experimental analysis discloses the robustness of the proposed approach and its capabilities in reacting to the malicious attack effects.

This provides an important way for us to analyze network attack nodes. Based on a previous study [42], it analyzed the probability of a node failure due to different attack methods. In this paper, the authors do not introduce specific details, but only consider the results after the nodes are deleted under attack. In this way, the paper lists 10 main attack methods to analyze the node failure of SBIN. The attack names and their physical meanings are shown in Table 3.

4.2. Study in Attack Information Metric Index

Based on the principle of graph theory, the following two problems should be considered for node attacks on the entire SBIN:

1. Breadth of attack information, that is, how many nodes are to be attacked; we introduce parameter α to indicate the breadth of attack information.

For the space-based information network, the node set that consists of the network is V, and the total number of nodes is N. Therefore, the capacity of the attack sample can be expressed as:

$$n = N\alpha, \alpha \in [0, 1] \tag{2}$$

The larger α is, the higher the breadth of attack information, and the higher the number of network nodes that will be attacked.

Table 3. Names and meanings of attacking node ways.

Identification	Name	Meaning
$\mathbf{A_1}$	Physical node attack	The physical destruction of the terminal node is performed by various means such as tearing, scratching, and high temperature.
$\mathbf{A_2}$	Transmission signal analysis	Crack the encryption information by algorithm, and then analyze the information characteristics to determine the data type and effect.
$\mathbf{A_3}$	Signal interception and node reconstruction	The node is reconstructed by tapping the communication data of the network node to acquire sensitive information in the channel.
$\mathbf{A_4}$	Communication interference	Block all levels of nodes from receiving normal communication signals, resulting in a link interruption by using flooding attacks, wormhole attacks, etc.
$\mathbf{A_5}$	Network Protocol Attack	Through pseudo-terminal technology, send random data that receiving nodes cannot identify, parse, and recover.It also sends malformed data causing a crash.
$\mathbf{A_6}$	Spurious data injection	Send false information that completely complies with the communication mechanism and network protocol so that it can process and distribute false information.
$\mathbf{A_7}$	Wireless RF injection	Send information of virus-carrying, Trojans, or other malicious programs that fully comply with the communication mechanism and network protocol, and inject it into the data processing system to infect hosts, industrial computers, etc.
$\mathbf{A_8}$	Data copying, tampering, and deletion	Use the injected malicious code and software vulnerabilities to complete the copying, tampering, and deletion on the target database.
$\mathbf{A_9}$	Network paralysis	Cause the entire network data to lose normal application pass rates by maliciously attackingmultiple pseudo-terminals.
$\mathbf{A_{10}}$	Illegal control	Obtain root privileges of the system and achieve complete control of the system, including system operation, service provision, network management, etc.

2. The accuracy of the attack information, meaning which nodes should be attacked; we introduce parameter δ to represent the accuracy of the attack information. To eliminate multiple injections of highly important nodes, the node extraction process is designed to be a no return unequal probability sampling.

For the accuracy study of attack information, the order of importance of the nodes is first introduced. The auxiliary variable of the node v_i is:

$$\pi_i = r_i^{-\delta} \tag{3}$$

r_i denotes the sequence number for the importance of the node v_i; thus, under one sampling, the probability of the injection of the node is:

$$\nabla_i = \frac{\pi_i}{\sum_{t=1}^{N} \pi_t} = \frac{r_i^{-\delta}}{\sum_{t=1}^{N} r_t^{-\delta}} \tag{4}$$

It can be inferred that the larger δ is, the more likely that the important nodes are to be extracted, that is, the higher the accuracy of the node attack information. There exist two extreme situations, as follows:

(1) When $\delta = 0$,

$$\nabla_i = \frac{r_i^{-\delta}}{\sum_{t=1}^{N} r_t^{-\delta}} = \frac{1}{N} \tag{5}$$

In this condition, the probability that the node is to be extracted is the same, and the attack information is called random information.

(2) When $\delta = \infty$,

$$\sum_{t=1}^{N} r_t^{-\infty} = \sum_{t=1}^{N} t^{-\infty} = 1 + \sum_{t=2}^{N} t^{-\infty} = 1 \tag{6}$$

Assume that $r_{i*} = 1$

$$\nabla_i = \begin{cases} \frac{1}{\sum_{t=1}^{N} r_t^{-\delta}} = 1 & i = i* \\ \frac{1}{\sum_{t=1}^{N} r_t^{-\delta}} = 0 & i \neq i* \end{cases} \tag{7}$$

In this condition, the most important node is always preferentially extracted, and this attack information is called priority information.

4.3. Attack Strategy Algorithm Research

At present, mainstream research on the node attack strategy method is mainly composed of two parts: the traditional attack strategy and the tree attack strategy. The traditional attack strategy sorts the rules according to the metric indexes of the attack nodes, selects the target nodes according to the proposed order and implements the attacks (see Figure 4a); the tree attack strategy is based on the extension of the tree root-branch-leaf to implement an attack on a selected target node (see Figure 4b). The specific analysis is as follows.

1. Traditional attack strategy (TAS):

   (1) Select node degree metric index to analyze the invulnerability of SBIN;
   (2) Select the attack node according to the breadth and accuracy of the attack information;
   (3) Attack the relevant nodes of SBIN in the appropriate steps according to the attack ratio;
   (4) Statistical metric index and perform a data analysis.

2. Improved tree-attack strategy (ITAS):

   (1) Define the degree of the node as a measure index, selecting the non-isolated node in the network as a root node by a certain attack breadth and accuracy;
   (2) Invade all of the neighboring nodes of the root node as second layer nodes;
   (3) In the process of proportional deletion, the order of deletion is performed according to the root node, the root sibling node, the branch node, and the branch sibling node;

(4) Attack the adjacent nodes of all of the second-layer nodes successively as third-layer nodes of the improved tree attack strategy until all nodes in SBIN are traversed.

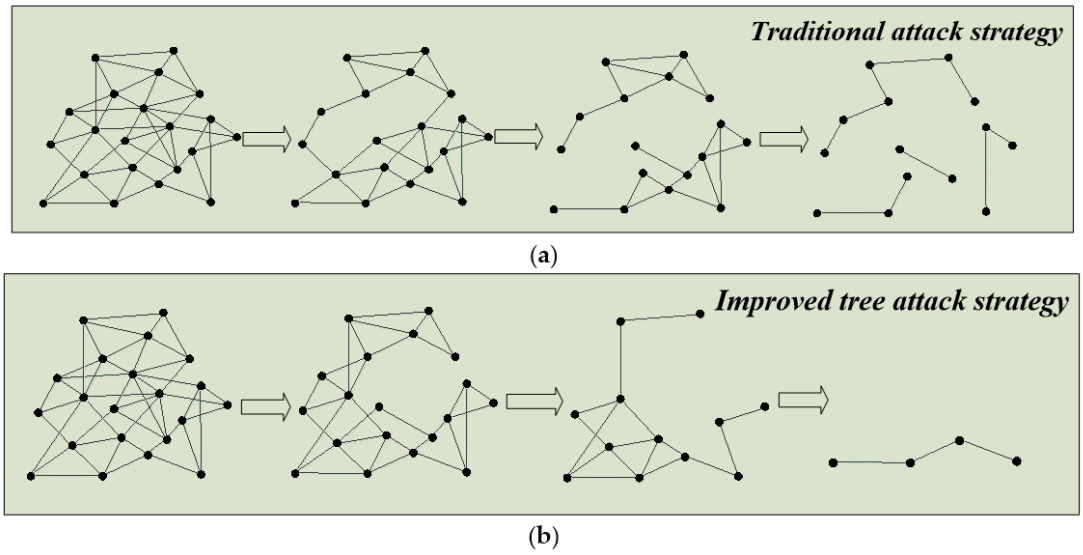

Figure 4. (**a**) Schematic diagram of the traditional attack strategy, (**b**) Schematic diagram of the improved tree attack strategy.

4.4. Invulnerability Metric Index

1. Betweenness centrality of nodes

The betweenness centrality of nodes is a metric index to evaluate the importance of nodes in the network. BC_i is usually used to represent the betweenness centrality of node v_i. The larger BC_i is, the higher the number of shortest paths through the node v_i in the whole network. Therefore, node v_i is more important.

$$BC_i = \sum_{s \neq i \neq t} \frac{n_{st}^i}{g_{st}} \tag{8}$$

Among them, g_{st} is the number of shortest paths from node s to node t, and n_{st} is the number of shortest paths through node i in the g_{st} shortest paths from node s to node t.

2. Maximum connected subgraph

In the construction of the SBIN model, we use $G = \langle V, E \rangle$ to describe the mapping relationship between the nodes and connected edges of the entire network. In the connected graph $G = \langle V, E \rangle$, if there is a subgraph $G' = \langle V', E' \rangle$ and $V' \subseteq V, E' \subseteq E$, then G' is the connected subgraph of G. In the multiple connected subgraphs of the network G, the connected subgraph with the largest number of nodes is considered as the maximal connected subgraph.

3. Invulnerability metric index

Definition: *N is the initial number of nodes in the whole network. N' is the number of nodes in the maximal connected subgraph after the attack; the invulnerability metric index S is:*

$$S = \frac{N'}{N} \tag{9}$$

5. Invulnerability Optimization Model of SBIN

The edge-increasing method refers to the method of optimizing the invulnerability of the system by adding a certain proportion of connected edges in SBIN. Based on the measurement index of the complex network, four different edge-increasing methods are designed to optimize the invulnerability of SBIN. An appropriate edge-increasing ratio is defined, and on this basis, a simulation experiment is carried out for each edge-increasing strategy to analyze the optimization effect.

5.1. Analysis Index of Invulnerability in SBIN

In this paper, four types of edge-increasing strategies are designed, and the edge to be added should be limited to a certain proportion. We assume that N_a indicates the total number of edges to be added, while I indicates the total number of edges that have been added. In the four edge-increasing strategies, all edges are added one by one, and the network parameters need to be recalculated after each increase of a certain proportion. In the paper, the edge-increasing ratio is defined as:

$$f_a = N_a / m_0 \tag{10}$$

Among them, m_0 represents the total number of edges in the initial network.

5.2. Optimization Methods of Invulnerability in SBIN

1. Random edge-increasing method (RD).

   Step 1: Initialize $i = 0$, and abstract the SBIN into the graph $G = (V, E)$;
   Step 2: Randomly select two nodes with no edges connected in the graph G, the graph after adding the edge is G', set $i = i + 1$ and $G = G'$;
   Step 3: If $i \leq N_a$, go back to step 2 and continue to increase the edge until the end of the edge increasing process;
   Step 4: Calculate the BC_i of all nodes and the maximum value $BC_{\max}$ in SBIN after adding the N_a edges.

2. Low nodes degree with high priority (LDF).

   Step 1: Initialize $i = 0$, and abstract the SBIN into the graph $G = (V, E)$;
   Step 2: Arrange all nodes in SBIN from small to large according to the degree value;
   Step 3: Select two nodes with the smallest degree value and no edges connected in the graph G, the graph after adding the edge is G', set $i = i + 1$ and $G = G'$;
   Step 4: If $i \leq N_a$, go back to step 2, or go to step 5;
   Step 5: Calculate the BC_i of all nodes and the maximum value $BC_{\max}$ in SBIN after adding the N_a edges.

3. Low nodes betweenness centrality with high priority (LBF).

   Step 1: Initialize $i = 0$, and abstract the SBIN into the graph $G = (V, E)$;
   Step 2: Arrange all nodes in SBIN from small to large according to the betweenness centrality value;
   Step 3: Select two nodes with the smallest betweenness centrality value and no edges connected in the graph G, the graph after adding the edge is G', set $i = i + 1$ and $G = G'$;
   Step 4: If $i \leq N_a$, go back to step 2, or go to step 5;
   Step 5: Calculate the BC_i of all nodes and the maximum value $BC_{\max}$ in SBIN after adding the N_a edges.

4. Adding shortcut in nodes with the maximum betweenness centrality method (SMB).

As shown in Figure 5 below, node 1 is the central node, and its neighbor nodes are node 2, node 3, and node 4. The number next to the dotted line between the neighboring nodes indicates the number

of shortest paths passing through 3 nodes at the same time. If one selects two neighbor nodes with the largest betweenness centrality value among all the edges adjacent to the central node and add an edge between them, some of the shortest paths will no longer pass through the central node.

Step 1: Initialize $i = 0$, and abstract the SBIN into the graph $G = (V, E)$;
Step 2: Calculate the betweenness centrality value of all nodes in SBIN, find the node with the largest betweenness centrality value $v_{BC_{\max}}$, and the edge set $Ev_{BC_{\max}}$ connected to the node $v_{BC_{\max}}$;
Step 3: Sort the betweenness centrality value of all the edges in the order from largest to smallest, and record the corresponding node set as $O_{v_{BC_{\max}}}$ at the other end of these edges;
Step 4: Select the two nodes with no edges connected in the top from $O_{v_{BC_{\max}}}$, add an edge between the nodes, the graph after adding the edge is G', set $i = i + 1$ and $G = G'$;
Step 5: If $i \leq N_a$, go back to step 2, or go to step 6;
Step 6: Calculate the BC_i of all nodes and the maximum value $BC_{\max}$ in SBIN after adding the N_a edges.

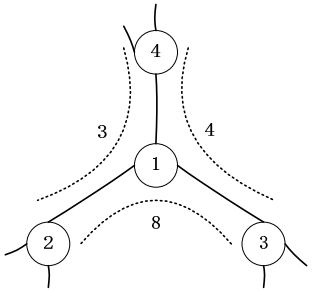

Figure 5. Analysis diagram of adding a shortcut.

6. Experimental Section and Analysis

6.1. Comparison Experiments of Invulnerability Analysis

Based on the definition of the attack information metric index and strategy algorithm, we carry out the simulation analysis of SBIN. First, the maximum connected subgraph is selected as the metric index to measure the effect before and after the network attack. Second, under the traditional attack strategy and the improved tree attack strategy, we set different attack information breadth and accuracy parameters, and delete the selected node and the connected edge according to the unequal probability sampling rule. We analyze the invulnerability effect of different strategies on SBIN. Finally, the paper compares the advantages and disadvantages of the two attack modes under the condition that the parameters are the same but the strategies are different. In this paper, 20 experiments were carried out independently, and the mean value of the invulnerability measurement index was calculated last, verifying the universality of the simulation results.

1. Invulnerability analysis under different values of the attack accuracy of the traditional attack strategy

In the process of analyzing the invulnerability under different values of the attack accuracy based on the traditional attack strategies, the attack breadth was first quantitatively controlled. With the increase of the attack breadth, more and more nodes had been attacked in SBIN. The number of its deleted nodes also increases gradually, which directly leads to a decrease of invulnerability and makes the whole simulation curve show a downward trend.

Under the condition of a certain attack breadth, the attack accuracy of $\delta = 0$, $\delta = 2$ and $\delta = 10$ are studied respectively. When $\delta = 0$, the selected attack nodes are random. Therefore, the whole

network is in a state of random failure under the traditional attack strategy, and the performance of the related nodes and connection edges tends to be flat with the increase of the attack breadth. When $\delta = 10$, the whole network presents a sharp downward trend at the very beginning. Because the attack accuracy increases, the selected network node was the node with the larger characteristic parameters in the whole network. When these nodes were attacked and deleted, the connected edges were deleted. This makes the whole network invulnerability reduce rapidly. In the research process of this paper, we found that when the attack accuracy increases to $\delta = 20$, the change scope is close to $\delta = 10$. Consequently, it can be considered that the node attack accuracy of $\delta = 10$ belongs to a deliberate attack, which directly leads to the decline of the invulnerability of the whole network.

Figure 6 shows that the schematic diagram of the invulnerability of SBIN changes with the increase of the attack breadth in the traditional attack strategy, at the different values of the attack accuracy; the relevant data analysis is shown in Table 4.

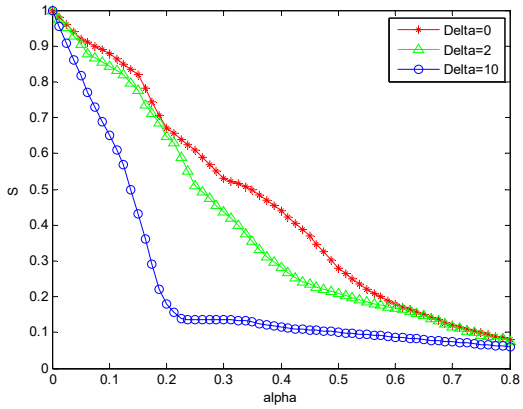

Figure 6. Invulnerability analysis of the traditional attack strategy under different values of the attack accuracy.

Table 4. Statistical table of the traditional attack strategy data under different values of the attack accuracy.

	$\delta = 0$	$\delta = 2$	$\delta = 10$
$\alpha = 0.05$	0.92	0.904	0.816
$\alpha = 0.1$	0.88	0.844	0.65
$\alpha = 0.15$	0.82	0.776	0.43
$\alpha = 0.2$	0.67	0.648	0.18
$\alpha = 0.25$	0.61	0.51	0.1365
$\alpha = 0.3$	0.53	0.438	0.1357
$\alpha = 0.35$	0.5	0.354	0.1311
$\alpha = 0.4$	0.44	0.282	0.1144
$\alpha = 0.45$	0.37	0.234	0.1077
$\alpha = 0.5$	0.28	0.21	0.1009
$\alpha = 0.55$	0.22	0.186	0.0941
$\alpha = 0.6$	0.18	0.168	0.0873
$\alpha = 0.65$	0.15	0.148	0.0805
$\alpha = 0.7$	0.12	0.116	0.0737
$\alpha = 0.75$	0.1	0.091	0.0669
$\alpha = 0.8$	0.08	0.076	0.06

2. Invulnerability analysis of different attack strategies in $\delta = 10$

As the 'ulcerative' results appearing under the traditional attack strategy indicate, although the invulnerability declines to some extent, the attacked network composed of the largest connected

subgraph may not be capable of performing related tasks. Therefore, our paper proposes an improved tree attack strategy to get add a further simulation comparison experiment.

Both of the attacks are performed based on deliberate attacks in $\delta = 10$. With the breadth of the attacks increasing, the two attack strategies present different experimental results. As shown in Figure 7, the traditional attack strategy first has a faster deteriorating trend than the improved tree attack strategy. However, with the attack breadth increasing, the first cross point appears between the two curves. It shows that on the condition of a small attack breadth, the traditional attack strategy tends to attack the node with large characteristic parameters, and its attack situation is an "ulcerative" development. Meanwhile, in the improved tree attack strategy, the secondary attack would be performed on the branch node connected to the root node. Therefore, under the condition of a lower attack breadth, its invulnerability is higher than for the traditional attack strategy. As the breadth of the attacks increases, the second cross point appears between the two attack strategies. In the attack process between the first and second cross points, due to the organizational structure and the connecting relationship of SBIN studied in this paper, the invulnerability of the improved tree attack strategy is significantly reduced. This result proves that the degree of nodes connected to the root node or the root sibling node is low. When the root node or the root sibling node is attacked, the nodes with smaller degrees will be attacked, making the invulnerability of the whole network decline rapidly. This also proves the effectiveness of the improved tree attack strategy. Since the improved tree attack strategy implements a layering and an attack based on the node connection relationship, when the attack breadth $\alpha > 0.2$, the invulnerability metric based on the improved tree attack strategy is smoothed down, while the invulnerability metric of the traditional attack strategies drops significantly. This is because the attacking node in the improved tree attack strategy becomes the node with a large degree, while the traditional attack strategy keeps attacking the related nodes proportionally. Therefore, it brings more damages to the entire network than the improved tree attack strategy does. Finally, when the attack breadth reaches 0.75, the invulnerability of the whole network under the improved tree attack strategy reduces to 0. This indicates that there exist almost no interconnected nodes in the network, so it cannot complete any related SBIN tasks. This is more practical than the traditional attack strategy, which cannot achieve the task function even if there are interconnected edges.

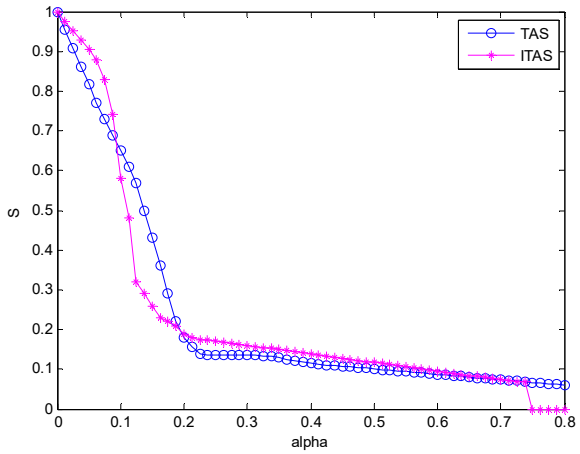

Figure 7. Invulnerability analysis under different attack strategies $\delta = 10$.

Figure 7 shows the invulnerability analysis of SBIN under different attack strategies, while the relevant data analysis is shown in Table 5.

Table 5. Data statistics under different attack strategies $\delta = 10$.

	TAS	**ITAS**
$\alpha = 0.05$	0.816	0.904
$\alpha = 0.1$	0.65	0.58
$\alpha = 0.15$	0.43	0.26
$\alpha = 0.2$	0.18	0.19
$\alpha = 0.25$	0.1365	0.171
$\alpha = 0.3$	0.1357	0.16
$\alpha = 0.35$	0.1311	0.149
$\alpha = 0.4$	0.1144	0.1386
$\alpha = 0.45$	0.1077	0.1278
$\alpha = 0.5$	0.1009	0.117
$\alpha = 0.55$	0.0941	0.1062
$\alpha = 0.6$	0.0873	0.0954
$\alpha = 0.65$	0.0805	0.0846
$\alpha = 0.7$	0.0737	0.0738
$\alpha = 0.75$	0.0669	0
$\alpha = 0.8$	0.06	0

6.2. Experiment of Invulnerability Optimization Analysis

To study the influence of the edge-increasing optimization method on the invulnerability of SBIN, this section mainly studies the comparative analysis of the invulnerability changes under four different edge-increasing strategies to the initial network, respectively. In this section, four kinds of edge-increasing ratio parameters, fa = 0.025, fa = 0.05, fa = 0.075, and fa = 0.1, are set. We proportionally delete the nodes through the improved tree attack strategy, and analyze the invulnerability changes under the four edge-increasing strategies RD, SMB, LBF and LDF.

As shown in Figure 8a, the invulnerability of SBIN increases with a greater edge-increasing proportion in the random edge-increasing strategy. This indicates that, in SBIN, a greater proportion of random increased edges means a greater average connectivity of the network nodes. When a node is deleted under the improved tree attack strategy, due to the increase of the average connectivity, the connectivity of the other nodes connected to the node is less affected than in the situation where no edges are added. Therefore, under the same deletion ratio, a larger random edge-increasing proportion brings a higher invulnerability metric and stronger invulnerability of SBIN.

As shown in Figure 8b, with a greater edge-increasing proportion in the SMB edge-increasing strategy, there are no significant changes in the invulnerability of SBIN. This is because SMB's edge-increasing strategy involves increasing the edge between adjacent nodes by a large degree, and the improved tree attack strategy deletes nodes according to the degree-betweenness centrality, precisely. Therefore, even if the number of connected nodes is increased for adjacent nodes, the invulnerability basically stays unchanged with the deletion of the nodes. Therefore, the SMB edge-increasing strategy is not suitable to be applied for invulnerability optimization under the improved tree attack strategy.

Figure 8c,d shows a comparative analysis of the impact on invulnerability under the LBF and LDF edge-increasing strategies.

It can be concluded from Figure 8c that the LBF edge-increasing strategy gets a better optimization result than the RD edge-increasing strategy. This is because adding edges between nodes with a low betweenness centrality increases the average betweenness centrality of the entire network, making the entire network have a higher number of shortest paths. When a node is attacked, the function of the network can be kept through the added edges. Therefore, the LBF edge-increasing strategy is better than RD. In Figure 8d, the LDF edge-increasing strategy is the most sensitive among the four edge-increasing strategies. The reason for this is that after the edge is added between the nodes with a low degree, the relevant nodes that are attacked in the improved tree attack strategy are not deleted because of the disconnection, and the function continues to be performed through the added edge. The LDF edge-increasing strategy theoretically increases the degree of the entire network, making the

whole network flatten, and the gap between the large degree nodes and small degree nodes is further narrowed; hence, the entire network is more resistant to destruction.

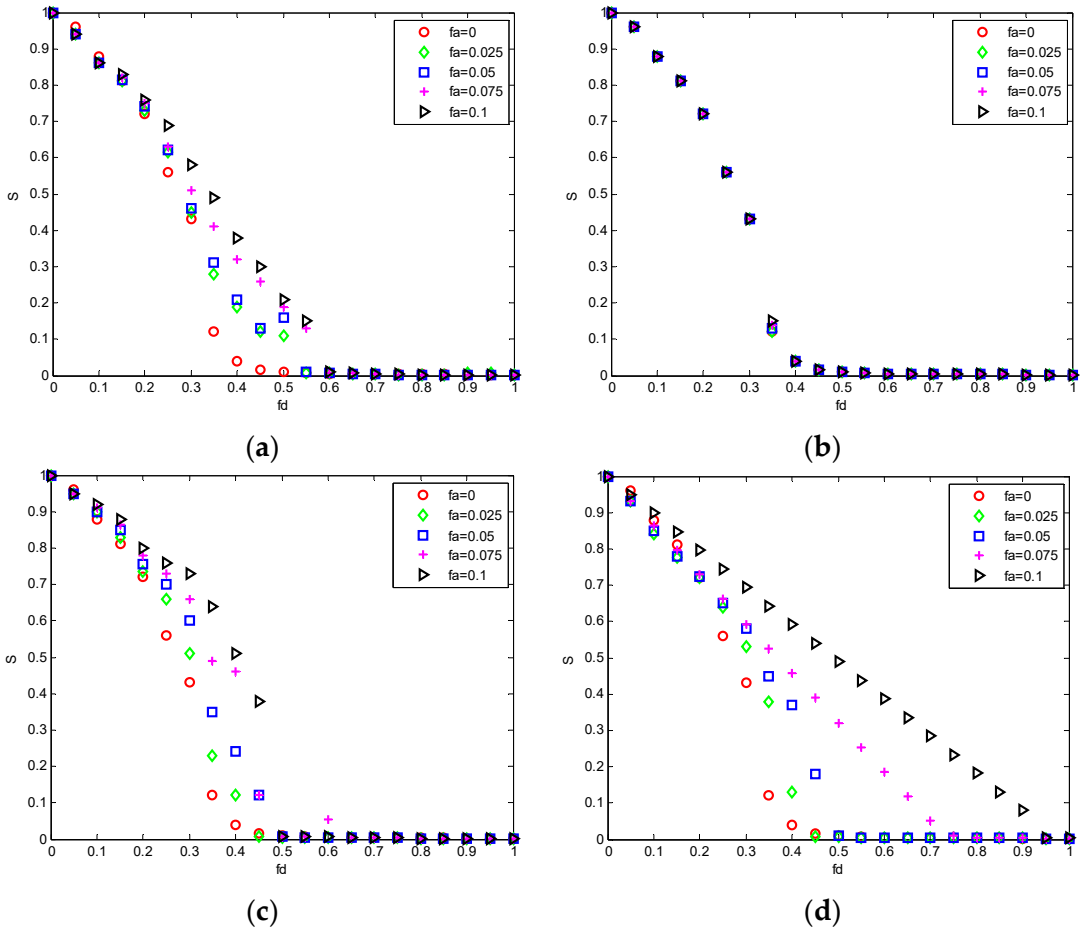

Figure 8. (**a**) RD edge-increasing strategy; (**b**) SMB edge-increasing strategy; (**c**) LBF edge-increasing strategy; and (**d**) LDF edge-increasing strategy.

After analyzing the invulnerability optimization results of different edge-increasing strategies under different ratios, this paper further studies the data of each edge-increasing strategy under the condition of an increasing edge ratio fa = 0.1, as shown in Figure 9.

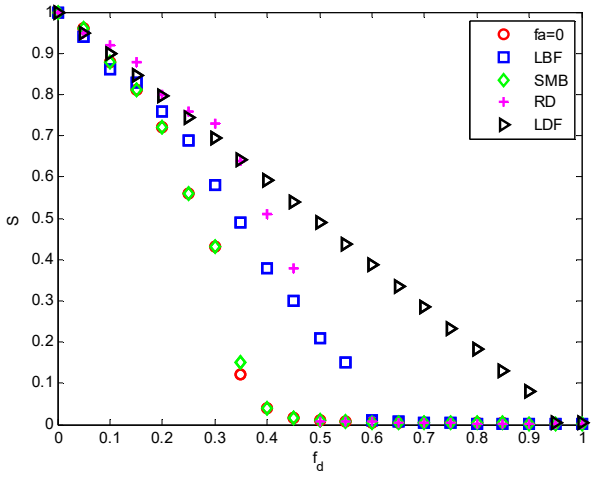

Figure 9. Invulnerability variation diagram of each edge-increasing strategy.

It can be concluded from the comparison that the SMB edge-increasing strategy has no obvious optimization effect on the invulnerability of SBIN. When the deletion ratio of SBIN is 50%, the invulnerability metric of the RD edge-increasing strategy is zero, which indicates that the connectivity of the entire system is basically zero; meanwhile, when the invulnerability of the LBF edge-increasing strategy is zero, the deletion ratio of the entire network comes to 60%, which means that the LBF edge-increasing strategy is more effective than RD; for the LDF edge-increasing strategy, when the invulnerability metric is zero, the number of deleted nodes in the entire network takes up 95%, that is, the LDF edge-increasing strategy has a high invulnerability application value under the condition that the entire network connection relationship is not completely deleted. In SBIN, an appropriate edge-increasing between nodes with a small degree can reduce the degree gap between nodes with large and small degrees, rendering the entire network flattened and evolved to resist the entire network. This has important theoretical support for the construction of a reasonably stable SBIN. The simulation and data analyses are shown in Figure 9 and Table 6.

Table 6. Simulation data of different edge-increasing strategies.

	fa = 0	**RD (fa = 1)**	**SMB (fa = 1)**	**LBF (fa = 1)**	**LDF (fa = 1)**
fd = 0	1	1	1	1	1
fd = 0.05	0.96	0.94	0.96	0.95	0.949
fd = 0.1	0.88	0.86	0.88	0.92	0.898
fd = 0.15	0.81	0.83	0.81	0.88	0.847
fd = 0.2	0.72	0.76	0.72	0.8	0.796
fd = 0.25	0.56	0.69	0.56	0.76	0.744
fd = 0.3	0.43	0.58	0.43	0.73	0.693
fd = 0.35	0.12	0.49	0.15	0.64	0.642
fd = 0.4	0.04	0.38	0.04	0.51	0.591
fd = 0.45	0.015	0.3	0.015	0.38	0.54
fd = 0.5	0.01	0.21	0.01	0.01	0.489
fd = 0.55	0	0.15	0	0	0.438
fd = 0.6	0	0.01	0	0	0.387
fd = 0.65	0	0.007	0	0	0.336
fd = 0.7	0	0	0	0	0.284
fd = 0.75	0	0	0	0	0.233
fd = 0.8	0	0	0	0	0.182
fd = 0.85	0	0	0	0	0.131
fd = 0.9	0	0	0	0	0.08
fd = 0.95	0	0	0	0	0
fd = 1	0	0	0	0	0

7. Conclusions

In this paper, the invulnerability of the relevant nodes of SBIN under different attack strategies is studied in depth, and the invulnerability of the network is optimized by adding edges, based on the complex network theory. First, the composition and function of SBIN are defined by constructing a reasonable network model and conducting a parameter analysis. Based on this, due to the low degree invulnerability of the traditional attack strategy, and due to the node that is connected but unable to perform tasks, this paper puts forward an improved tree attack strategy to analyse the invulnerability of SBIN before and after a node attack. By constructing a reasonable simulation model, the two attack strategies are studied, and the validity and feasibility of the algorithm are verified. Furthermore, on the basis of the analysis results, the invulnerability of the network is optimized by studying different edge-increasing strategies.

The paper is mainly aimed at the node attack model, and the next step is to try to study the invulnerability technology of the attack edge and the network model of the node and edges combination. In addition, we are preparing to continue to study the cascading failure caused in networks. These problems urgently need to be solved for the invulnerability in SBIN, so as to form a more complete

analysis system of invulnerability and in order to provide more reasonable technical support for the construction of SBIN.

Author Contributions: C.L. conceived and designed the method; W.X. guided the students to complete the research; C.L. performed the simulation and experiment tests; Y.Z., Y.S., C.G., and M.X. helped in the simulation and experiment tests; and C.L. wrote the paper.

Funding: The authors are grateful for the financial support received from the State 863 Project of China (No. 2014AA7116082) and the Fund Project of Science and Technology on Complex Electronic System Simulation Laboratory (No. 6142010XXXX002).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zhang, Y.; Xiao, X.; Chen, J. Impact of Information Network Damage on Overload-based Cascading Failures of Power Grid. *Autom. Electr. Power Syst.* **2017**, *41*, 14–21.
2. Ryzhov, Y.; Sakovych, L.; Vankevych, P.; Yakovlev, M.; Nastishin, Y. Optimization of requirements for measuring instruments at metrological service of communication tools. *Measurement* **2018**, *123*, 19–25. [CrossRef]
3. Knorr, F.; Baselt, D.; Schreckenberg, M. Reducing Traffic Jams via VANETs. *IEEE Trans. Veh. Technol.* **2012**, *61*, 3490–3498. [CrossRef]
4. Schurkus, H.F.; Luenser, A.; Ochsenfeld, C. Communication: Almost error-free resolution-of-the-identity correlation methods by null space removal of the particle-hole interactions. *J. Chem. Phys.* **2017**, *146*, 211106. [CrossRef]
5. Shcherbinin, A.G.; Mansurov, A.S. Numerical studies of the electromagnetic reciprocal influences of symmetric communication cable. *Russ. Electr. Eng.* **2014**, *85*, 673–676. [CrossRef]
6. Popovski, P.; Nielsen, J.J.; Stefanovic, C.; De Carvalho, E.; Ström, E.; Trillingsgaard, K.F.; Bana, A.-S.; Kim, D.M.; Kotaba, R.; Park, J.; et al. Wireless Access for Ultra-Reliable Low-Latency Communication: Principles and Building Blocks. *IEEE Netw.* **2018**, *32*, 16–23. [CrossRef]
7. Wang, K.; Shao, Y.; Shu, L.; Zhu, C.; Zhang, Y. Mobile big data fault-tolerant processing for ehealth networks. *IEEE Netw.* **2016**, *30*, 36–42. [CrossRef]
8. Guo, Q.; Yan, J.; Xu, W. Localized Fault Tolerant Algorithm Based on Node Movement Freedom Degree in Flying Ad Hoc Networks. *Symmetry* **2019**, *11*, 106. [CrossRef]
9. Vespignani, A. Complex networks: The fragility of interdependency. *Nature* **2010**, *464*, 984. [CrossRef]
10. Nepusz, T.; Vicsek, T. Controlling edge dynamics in complex networks. *Nat. Phys.* **2011**, *8*, 568–573. [CrossRef]
11. Krioukov, D.; Papadopoulos, F.; Kitsak, M.; Vahdat, A.; Boguñá, M. Hyperbolic geometry of complex networks. *Physics E* **2010**, *82*, 36106. [CrossRef]
12. Li, S.B.; Cao, D.N.; Dang, W.X. Variable speed limit strategies analysis with mesoscopic traffic flow model based on complex networks. *Int. J. Mod. Phys. C* **2018**, *29*, 1850014. [CrossRef]
13. Reiss, K.; Morzan, U.N.; Grigas, A.T.; Batista, V.S. Water Network Dynamics Next to the Oxygen-Evolving Complex of Photosystem II. *Inorganics* **2019**, *7*, 39. [CrossRef]
14. Memon, B.A.; Yao, H. Structural Change and Dynamics of Pakistan Stock Market During Crisis: A Complex Network Perspective. *Entropy* **2019**, *21*, 248. [CrossRef]
15. Wang, P.; Xue, F.; Li, H. A Multi-Objective DV-Hop Localization Algorithm Based on NSGA-II in Internet of Things. *Mathematics* **2019**, *7*, 184. [CrossRef]
16. Li, T.; Bai, J.; Yang, X. Co-Occurrence Network of High-Frequency Words in the Bioinformatics Literature: Structural Characteristics and Evolution. *Appl. Sci.* **2018**, *8*, 1994. [CrossRef]
17. Ding, C.; Yang, L.; Wu, M. Localization-Free Detection of Replica Node Attacks in Wireless Sensor Networks Using Similarity Estimation with Group Deployment Knowledge. *Sensors* **2017**, *17*, 160. [CrossRef]
18. Wan, J.; Xiong, N.; Zhang, W.; Zhang, Q.; Wan, Z. Prioritized Degree Distribution in Wireless Sensor Networks with a Network Coded Data Collection Method. *Sensors* **2012**, *12*, 17128–17154. [CrossRef]
19. Zhang, Y.; Na, S. Research on the Topological Properties of Air Quality Index Based on a Complex Network. *Sustainability* **2018**, *10*, 1073. [CrossRef]

20. Kasprzyk, R.; Najgebauer, A.; Pierzchała, D. Modelling and Simulation of an Infection Disease in Social Networks. In Proceedings of the International Conference on Computational Collective Intelligence (ICCCI 2011), Gdynia, Poland, 21–23 September 2011; pp. 388–398.
21. Joshi, C.; Kumar, U. Security Testing and Assessment of Vulnerability Scanners in Quest of Current Information Security Landscape. *Int. J. Comput. Appl.* **2016**, *145*, 1–7. [CrossRef]
22. Joshi, C.; Singh, U.K.; Singh, S.K. ZDAR system: Defending against the unknown. *Int. J. Comput. Sci. Mob. Comput.* **2016**, *5*, 143–149.
23. Singh, U.K.; Joshi, C.; Sk, S. Zero day attacks defense technique for protecting system against unknown vulnerabilities. *Int. J. Sci. Res. Comput. Sci. Eng.* **2017**, *5*, 13–18.
24. Kumar, U.; Joshi, C. Quantifying Security Risk by Critical Network Vulnerabilities Assessment. *Int. J. Comput. Appl.* **2016**, *156*, 26–33. [CrossRef]
25. Kumar, U.; Joshi, C.; Gaud, N. Information Security Assessment by Quantifying Risk Level of Network Vulnerabilities. *Int. J. Comput. Appl.* **2016**, *156*, 37–44. [CrossRef]
26. Singh, U.K.; Joshi, C. Quantitative Security Risk Evaluation Using CVSS Metrics by Estimation of Frequency and Maturity of Exploit. In Proceedings of the World Congress on Engineering and Computer Science (WCECS 2016), San Francisco, CA, USA, 19–21 October 2016.
27. Joshi, C.; Singh, U.K. Information security risk management framework for university computing environment. *Int. J. Netw. Secur.* **2017**, *19*, 742–751.
28. Lan, M.; Han, H. Study on invulnerability measure based on community structure of complex networks. *Comput. Eng. Appl.* **2012**, *38*, 23–28.
29. Peng, X.; Hong, Y. Power-law-alterable SF networks' cascading invulnerability under intentional attack. In Proceedings of the 2012 2nd International Conference on Computer Science and Network Technology, Changchun, China, 29–31 December 2012. [CrossRef]
30. Tian, T.; Jun, W.U.; Tan, Y.J. Simulation Optimization for Invulnerability of Complex Networks Based on Natural Connectivity. *Complex Syst. Complex. Sci.* **2013**, *10*, 88–94.
31. Jiang, C.; Wang, X.; Wang, J.; Chen, H.-H.; Ren, Y. Security in space information networks. *IEEE Commun. Mag.* **2015**, *53*, 82–88. [CrossRef]
32. Wang, X.; Du, J.; Wang, J.; Zhang, Z.; Jiang, C.; Ren, Y. Key Issues of Security in Space-Based Information Network Review. In Proceedings of the International Conferences on Cyberspace Technology (CCT 2014), Beijing, China, 8–10 November 2014. [CrossRef]
33. Du, J.; Jiang, C.; Guo, Q.; Guizani, M.; Ren, Y. Cooperative earth observation through complex space information networks. *IEEE Wirel. Commun.* **2016**, *23*, 136–144. [CrossRef]
34. Du, J.; Jiang, C.; Wang, J.; Ren, Y.; Yu, S.; Han, Z. Resource Allocation in Space Multi-Access Systems. *IEEE Trans. Aerosp. Electron. Syst.* **2017**, *53*, 598–618. [CrossRef]
35. Wang, W.; Hu, B.; Di, P. Optimization of Network Invulnerability to Cascading Failure Based on Random-walk Betweenness Model. In Proceedings of the 2011 International Conference on Information Management, Innovation Management and Industrial Engineering (ICIII 2011), Shenzhen, China, 26–27 November 2011; pp. 231–234.
36. Chen, S.; Jiang, J.; Pang, S.; Nie, S.; Lai, Y. Modeling and Optimization of Train Scheduling Network Based on Invulnerability Analysis. *Appl. Math. Inf. Sci.* **2013**, *7*, 113–119. [CrossRef]
37. Li, F.; Hu, B.; Di, P. Optimization of dynamic invulnerability of scale-free networks based on limited resource model. *Syst. Eng. Electron.* **2012**, *34*, 175–178.
38. Petrillo, A.; Pescapé, A.; Santini, S. A collaborative approach for improving the security of vehicular scenarios: The case of platooning. *Comput. Commun.* **2018**, *122*, 59–75. [CrossRef]
39. Petrillo, A.; Salvi, A.; Santini, S.; Valente, A.S. Adaptive multi-agents synchronization for collaborative driving of autonomous vehicles with multiple communication delays. *Transp. Res. Part C Emerg. Technol.* **2018**, *86*, 372–392. [CrossRef]
40. Fiengo, G.; Petrillo, A.; Salvi, A.; Santini, S.; Tufo, M. A control strategy for reducing traffic waves in delayed vehicular networks. In Proceedings of the 2016 IEEE 55th Conference on Decision and Control (CDC), Las Vegas, NV, USA, 12–14 December 2016; pp. 2462–2467.

41. Petrillo, A.; Pescape, A.; Santini, S. A collaborative control strategy for platoons of autonomous vehicles in the presence of message falsification attacks. In Proceedings of the 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), Naples, Italy, 26–28 June 2017; pp. 110–115.
42. Liu, C.; Xiong, W. Research on Internet of Things Vulnerability Based on Complex Network Attack Model. In Proceedings of the 3rd International Conference on Space Information Network (SINC 2018), Changchun, China, 9–10 August 2018; pp. 21–29.