IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON PROXIMITY SERVICE (PROSE) CHALLENGES AND APPLICATIONS

Received December 15, 2018, accepted January 4, 2019, date of publication January 10, 2019, date of current version February 4, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2891505

Complex Attack Linkage Decision-Making in Edge Computing Networks

QIANMU LI[1,2], SHUNMEI MENG[2,3], SAINAN ZHANG[2], JUN HOU[2], AND LIANYONG QI[4]

[1]Intelligent Manufacturing Department, Wuyi University, Jiangmen 529020, China
[2]School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China
[3]State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210023, China
[4]School of Information Science and Engineering, Qufu Normal University, Rizhao 276826, China

Corresponding author: Lianyong Qi (lianyongqi@gmail.com)

This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant 30918012204, in part by the Jiangsu Province Key Research and Development Program under Grant BE2017739, in part by the Jiangsu Province Key Research and Development Program under Grant BE2017100, in part by the 2018 Jiangsu Province Major Technical Research Project "Information Security Simulation System" (electric power and energy), in part by the National Science Youth Foundation of China under Grant 61702264, in part by the Open Research Project of the State Key Laboratory of Novel Software Technology, Nanjing University, under Grant KFKT2017B07, and in part by the Natural Science Foundation of China under Grant 61872219.

ABSTRACT The edge computing network refers to a new paradigm of edge-side big data computing networks, which integrates networks, computing, storage, and business core capabilities. It is close to users, the Internet of Things (IoT), or data source side. The edge computing network is generated by the common development of cloud computing and the IoT. The core is the massive uplink monitoring collection and downlink decision-making control big data generated by intelligent sensing devices, solving the problem of low data computing efficiency and performance under the centralized cloud computing model. Compared with traditional cloud computing networks, the edge computing network has more abundant terminal types, more frequent data real-time interaction, more complex transmission network technology systems, and more intelligent and interconnected business systems. Moreover, this situation is aggravated with the mobile edge computing, e.g., model proximity service increasingly prevalent in daily life. However, the ubiquitous and open features of edge computing networks expose network security risks to all parts of the system, facing severe security protection challenges. To solve the linkage disposal and minimum cost response of complex attacks, we propose an attack linkage disposal decision-making method for edge computing network systems based on attribute attack graphs. A simplified attribute attack graph is constructed through the network security alarm association and false-alarm determination, and formal correlation analysis is performed on the causal relationship of the alarm information. On this basis, the linkage defense strategy decision computing is transformed into the minimum dominance set solution of the attribute attack graph. Finally, a linkage disposal strategy execution point decision algorithm based on the greedy algorithm is designed, which constructs a set of attack linkage disposal decision-making technologies with optimal defense cost. It provides a powerful guarantee for timely and effectively active defense.

INDEX TERMS Edge computing network, complex attack detection, attribute attack graph, linkage defense.

I. INTRODUCTION

In the edge computing network, the edge computing service system forms an edge distributed computing system with full-time domain airspace interconnection on the edge side with the sinking of computing power. The service system is interconnected with the main station service system in real time as well, leading to a large overall scale and complex structure. It thus exhibits mixed multi-scale dynamic characteristics and complex network characteristics. In the era of big data, user data is inevitable to be exposed to the public, which leads to the threats of privacy invasion. Therefore, many privacy protection methods were proposed to defend the data attacks [1]–[3]. However, a large number of network security monitoring alarm data is still generated in the system domain of the edge computing network [4]. Taking the electric power domain as an example, 10 TB of network security event big data is generated every day. These alarm data for the network attack event has big data characteristics

(e.g., massive, diverse, heterogeneous, and dynamic changes) [5]. For one hand, analyzing and processing the network attack events effectively and efficiently are the difficult challenges. On the other hand, because of the existence of complex multi-point network attacks, network alarm information has causal logical relevance (e.g., mobile proximity service), and how to mine complex attack processes for minimum cost defense is also a difficult problem [6]–[8]. Currently, network security defense technologies based on alarm correlation and attack graphs are important methods for complex attack handling [9]. The alarm correlation technology is mainly applied to the discovery of multi-point and multi-step attack modes and provides an execution point decision mechanism for network linkage processing [10], [11]. In terms of alarm relationship extraction, the attack graph enumerates all possible attack paths and forms an attack sequence based on the comprehensive analysis of the vulnerability of each node in the network from the perspective of the attacker, thus providing alarm mapping and association analysis rules. At the same time, there are a large number of redundant alarms in the attack data. The network attack based on the alarm association and the attack graph has a state explosion problem. How to calculate the optimal attack linkage processing strategy for large-scale edge computing networks is an NP hard problem [12], [13].

To this end, this paper further proposes a joint action strategy decision generation method. It is based on the attribute attack graph of edge computing networks [14]. First, we associate the alarms based on the attribute association method to generate the reduced attribute attack graph. Second, for the attribute space explosion problem caused by the redundant alarm, the redundant alarm optimization processing method based on k-means analysis is proposed. The state space of the graph is further reduced. On this basis, the linkage treatment strategy calculation is transformed into the minimum dominance set of the attribute attack graph, and the decision-making space of the linkage processing strategy is refined. Then the decision-making algorithm based on the greedy algorithm is designed to determine the minimum cost linkage disposal strategy for large-scale systems of edge computing networks, effectively reducing the complexity and difficulty of this problem. Finally, the experimental results verify the effectiveness of the attack linkage strategy generation method based on the attribute attack graph and minimum dominance set. It is proved that the method can be applied to the minimum cost linkage processing of security events in the edge computing network environment. Figure 1 shows the relevant content of this study.

The rest of the paper is organized as follows: Section 2 introduces the research progress of related techniques of attribute attack graphs. Section 3 gives the attribute attack graphs and dominating set formal description definitions for complex attack linkage processing, and gives a method for refining linkage handling problems. In the section 4, the linkage processing decision model is given, and the edge computing network attack is modeled and analyzed through alarm correlation. The attribute attack graph construction and state space reduction algorithm are given. Section 5 proposes a network security linkage processing enforcement point and security policy generation algorithm based on attribute attack graph minimum dominance set (MDS) and offensive and defensive income. Section 6 verifies the effectiveness of the algorithm through simulation experiments. Section 7 summarizes the paper and gives relevant conclusions.

II. RELATED RESEARCH

At present, complex attack detection and defense technologies based on alarm correlation and attack analysis have received much attention in the security situation where complex attacks such as attack detection and threat assessment (APT) continue to evolve. For the first time, Swiler has proposed the graph model based attack in which the attack of adversary is supposed to an edge, and each node represents a network state [48]. The administrator can determine the key nodes of the network by calculating the probability of a successful attack. This attack graph is known as a state attack graph [15], [16]. The state attack graph technology is often used for network security situational awareness and assessment. Liu [17] proposed a method based on state attack graph for the APT in his dissertation. In this work, the state attack graph is used to correlate large-scale alarms as well as to conduct a multi-step attack situation threat assessment. Musa [18] proposed a network security attack graph analysis method for complex network environments. By combining

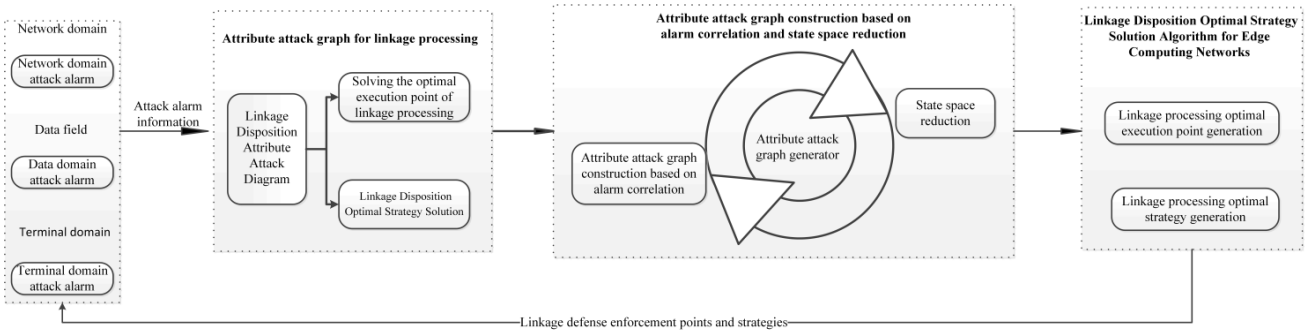


FIGURE 1. Technical framework for linkage decision-making of edge computing network systems.

large-scale alarm information and vulnerability information, an attack graph based on risk level assessment is generated to achieve network security assessment. Sheyner [19] proposed a network security event alarm correlation analysis method combining situational map and attack graph to analyze the network security risk situation. Chen *et al.* [20] proposed a network security metric based on the number of attack paths. Roschke *et al.* [21] proposed a network security metric based on the mean length of attack paths. Saurabh and Sairam [22] also proposed their own security metrics. However, the evaluation of network security is not significant, and it is not good to assist network administrators in making decisions. The advantage of the state attack graph is that it is easy for managers to intuitively understand the entire process of the attack to implement security defense. However, as the scale of the network is prone to state explosion problems, in order to solve this problem, Alhomidi and Reed [23] proposed a ''monotonic hypothesis'', which assumes that the target of the attack is developing in the direction of increasing attack power. That is, the attack capability that has been obtained is not repeatedly obtained, so the problem of attack correlation analysis in the case of a large number of false alarms and redundant alarms in the network cannot be solved.

In recent years, around the variants of the attack graph, the constructions of the attack graph and its various applications have produced a lot of research results [24]. For edge computing networks with large network scales, using attribute attack graphs for vulnerability analysis is a better way than using state attack graphs. Although there are some defects in visually understanding the attack trajectory, it can effectively solve the state explosion problems. On the basis of this, Noel and Jajodia [25] proposed an attribute attack graph model. There are two types of nodes in the attribute attack graph, one is the network security element and the other is the specific vulnerability point. Through such abstraction, it can effectively compress the scale of the attack graph. Wang *et al.* [26] proposed a network security defense method based on a minimal key set. But these methods do not take into account the complex relationship between attacks and network configuration elements. Li [27] also proposed a series of cybersecurity defense methods that destroy the initial conditions. However, these methods have the following shortcomings [15], [28], [29]: i) exponential solution space; ii) no cost consideration when selecting initial conditions to be destroyed; iii) no vulnerability fixes can be taken as network security defenses strategy. In order to solve the above problems, this paper proposes an edge computing network attack linkage decision-making technology using alarm correlation and attribute attack graphs.

III. ATTRIBUTE ATTACK MAP FOR LINKAGE PROCESSING

A. DEFINITION OF ATTRIBUTE ATTACK GRAPH FOR LINKAGE HANDLING

Aiming at the large-scale, complex and multi-point network attacks in the edge computing network, usually a reasonable edge computing terminal intrusion detection service is deployed in the edge computing network to implement distributed linkage intrusion detection. In this context, for the complex network attack alarm event handling problem generated by the edge computing network, this paper introduces attribute attack graph technology to link alarms.

Definition 1 (Atomic Attack Node:) It represents a single-step attack in the network, called an atomic attack node V_{atom}.

Definition 2 (Attribute Node:) Attribute node V_i^{pre} and V_i^{post} respectively represent the atomic attack node V_{atom} successful implementation of the premise attribute node and the consequence attribute node.

In the attribute attack graph, premise attribute nodes and consequence attribute nodes can be collectively referred to as attribute nodes. In addition, the attribute node can be further subdivided according to the network attack process. That is, in the attack process, there is a special attribute node, which is both the consequence attribute node of the atomic attack node V_{atom}^i and the premise attribute node of the V_{atom}^j, which becomes the intermediate process attribute node of the network attack. In addition, there is another attribute node in the attribute attack graph. Such attribute nodes exist only as premise attribute nodes, and not as the consequence attribute node of any atomic attack. Such nodes are called the initial attribute nodes of the attribute attack graph. According to the idea of active defense, any atomic attack cannot be implemented without the premise of the cyber-attack, and any subsequent associated attacks are not successfully implemented. Therefore, the initial attribute node becomes the key object of the active defense of cyber-attacks. In the network security defense work, the elimination of the initial attribute node can avoid a large part of the network attacks.

According to the graph theory, the initial attribute node is the most primitive condition of the attack, and its inbound edge is 0, and the outbound edge is greater than 1, so the initial attribute node has an in-degree of 0 and an out-degree is greater than or equal to 1 [30]. Similarly, an atomic attack node must have at least one prerequisite for successful implementation, so its entry degree is at least 1, and the degree of exit is 1. The consequence attribute node has an in-degree of at least 1. The details are shown in Table 1:

TABLE 1. Node accessibility condition.

Node u	id(u)	od(u)
Initial attribute node	0	$\geqslant 1$
Atomic attack	$\geqslant 1$	1
Consequence attribute node	$\geqslant 1$	$\geqslant 1/0$

Definition 3 (The Edge of the Attribute Attack Graph): E_{atom} represents the attack process of the atomic attack, which can be divided into the premise attribute edge $E_{atom}(V_i^{pre} \rightarrow V_{atom}^i)$ and the consequence attribute edge $E_{atom}(V_{atom}^i \rightarrow V_i^{post})$.

Definition 4 (Attribute Attack Graph): The attribute attack graph is defined as a directional and unweighted graph.

Given a point set $(V_i^{pre}, V_{atom}^i, V_i^{post})$ and an edge set $((V_i^{pre} \rightarrow V_{atom}^i), (V_{atom}^i \rightarrow V_i^{post}))$, the attribute attack graph can be defined as $AG = (V, E)$, where V represents the point set of the attribute attack graph, including the atomic attack node, premise attribute node, and consequence attribute node. E represents the edge set of the attribute attack graph, including the premise edge and the consequence edge.

The edge in the attribute attack graph may only point from the attribute node to the atomic attack node, or from the atomic attack node to the attribute node, and may not point to the attribute node from the attribute node, or the atomic attack node points to the atomic attack node, so the attribute attack graph can be treated as a weighted and directed bipartite graph. Furthermore, the nodes in the attribute attack graph can be divided into two sets: the atomic attack nodes represented by V_{atom} form a set, and the attribute node $V_{\text{attribute}}$ constitutes a set.

B. SOLVING THE OPTIMAL EXECUTION POINT OF LINKAGE PROCESSING BASED ON ATTRIBUTE ATTACK GRAPH

According to the definition of the attribute attack graph, the relationship between the initial attribute node and the atomic attack node in the network is a many-to-many relationship. Note that, in some cases, the atomic attack can only be performed when all of the premise attribute nodes of the atomic attack node are satisfied.

At the same time, there is also a situation in which an initial atomic attack can be performed when an initial attribute node can be successfully utilized. Given an initial set of attribute nodes $V_{\text{attribute}} = (V_{attribute}^a, V_{attribute}^b, V_{attribute}^c)$, assume that the initial attribute node $V_{attribute}^a$ is the premise attribute node of all atomic attack nodes, and $V_{attribute}^b, V_{attribute}^c$ is only the premise attribute node of the partial atomic attack nodes. In this case, the initial attribute node $V_{attribute}^a$ is called the optimal defense execution point. Because only the attribute node D needs to be securely reinforced, the defense against many atomic attacks can be implemented.

Therefore, in the complex network environment of the edge computing network, the advantage of introducing the attack graph technology for linkage defense processing is that it can use the graph to perform causal logical association of different alarm events, which can effectively find a complex multi-step attack. What's more, finding the initial attribute node in the attribute attack graph for targeted defense processing can greatly reduce the defense cost of the edge computing network. The following paper provides a formal description of the solution to the optimal defense enforcement point:

Definition 5 (Dominating Set): This is represented by DS. In the attribute attack graph $AG = (V, E)$, the node set $S \subseteq V$ is a dominating set of G.

Definition 6 (Minimal Dominating Sets): This is denoted by $DS'_{\min}$, and $DS'_{\min}$ is a minimal dominating set if and only for any $DS \in DS'_{\min}$, DS is no longer a dominating set.

Definition 7 (Minimum Dominance Set): This is represented by $DS_{\min}$, which is the minimum dominating set with the smallest base.

In this way, the optimal network linkage processing execution point selection problem is converted to solving the minimum dominating set formed by the initial attribute node set.

The main idea of solving the optimal network linkage processing execution point is to regard the attribute attack graph as a directed bipartite graph. Then decide what to do in the face of cyber-attacks by calculating the minimum dominance set (MDS) of the attribute attack graph AG which is composed of the initial attribute node. The resulting minimum dominating node represents a set of key attributes that cover all atomic attack nodes and can achieve effective cyber security defenses if these attributes are disabled.

The solution of the optimal linkage processing execution point is converted into a classic set coverage problem [31], [32]. Because each initial attribute node in the attribute attack graph AG can cover one or more atomic attack nodes, it can be assumed that all m atom attack nodes in the attribute attack graph G are divided into n subsets [33]. Each of the n subsets corresponds to a specific initial attribute node. One corresponds to a specific initial attribute node. The goal of this paper is to calculate the optimal coverage set of all atomic attack nodes in the attribute attack graph AG, which can cover all atomic attack nodes in the attribute attack graph and has the smallest number of initial attribute nodes.

Take a hypothetical target network as an example, and regard its corresponding attribute attack graph as a bipartite graph. As shown in Figure 2-a. The atomic attack node and the initial attribute node are the most important nodes in the attack graph, and the consequence attribute node is only the result of a successful atomic attack. Because the goal of this article is to calculate the MDS that can cover all atomic attacks in the initial attribute node-set, all the consequence attribute nodes in the bipartite graph can be removed. The bipartite diagram obtained by the above operation is shown in Figure 2-b. The figure only contains the initial attribute node, the atomic attack node, and the directed edge from the former to the latter. The MDS calculated in the resulting bipartite graph gives the set of the initial attribute nodes which overrides all atomic attacks in the attribute attack graph.

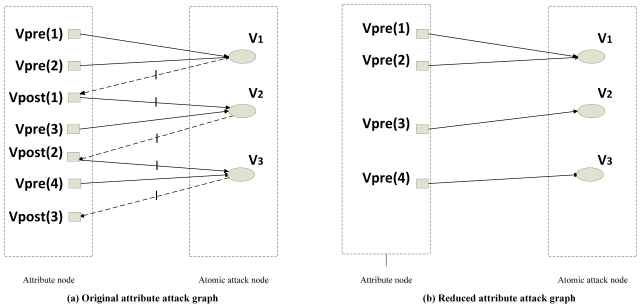


FIGURE 2. Bipartite graphs corresponding to the attribute attack graph.

C. LINKAGE DISPOSITION OPTIMAL STRATEGY SOLUTION

After obtaining the solution for selecting the optimal execution point of the edge computing network linkage processing, it is also necessary to solve the optimal strategy selection problem of linkage processing for the optimal execution point. From the perspective of network attack and defense, the attacker's attack action has certain randomness, so the generation of security alarm information in the edge computing network is also random [34], [35]. In this paper, the generation of attribute attack graphs based on network security alarms will also be affected by the alarm information. In the minimal dominance of attribute attack graphs for linkage handling, the attribute node and its associated attack hazard have a certain probability distribution.

In order to achieve optimal defense against complex attacks, it is necessary to select the defense strategy with the maximal defense benefit. The probability of successful implementation of the initial attribute node $V_{\text{attribute}}$ and the resulting overall hazard index distribution are represented by p_{pre} and u_{pre}. The overall hazard index can be obtained by accumulating the hazards of the initial attribute nodes in the minimum dominance set of the attribute attack graph. Define the probability distribution p_d and the defense gain u_d of cyber-attack defense strategy accordingly.

Given the minimum dominating set, the probability distribution of the initial attribute nodes is assumed to be:

$$p^i_{pre} = (p^i_{pre_1}, p^i_{pre_2}, L\, p^i_{pre_m}), \quad 0 \le p^i_{pre_j} \le 1, \ \sum_{j=1}^{m} p^i_{pre_j} = 1 \tag{1}$$

The probability distribution of the defense party selecting the defense strategy is:

$$p^i_d = (p^i_{d_1}, p^i_{d_2}, L\, p^i_{d_n}), \quad 0 \le p^i_{d_k} \le 1, \ \sum_{k=1}^{n} p^i_{d_k} = 1 \tag{2}$$

Then the game income of both offense and defense is expressed as:

$$pt^i_{pre}(p^i_{pre}, p^i_d) = \sum_{j}^{m} p^i_{pre_j} (\sum_{k}^{n} p^i_{d_k} u^i_{pre}) \tag{3}$$

$$pt^i_d(p^i_{pre}, p^i_d) = \sum_{k}^{n} p^i_{d_k} (\sum_{j}^{m} p^i_{pre_j} u^i_d) \tag{4}$$

On this basis, the optimal linkage treatment strategy $(p^{i\circ}_{pre}, p^{i\circ}_d)$ can be obtained by solving the Nash equilibrium condition. That is, for $\forall p^i_d$, there is:

$$pt^i_d(p^{i\circ}_{pre}, p^{i\circ}_d) \ge pt^i_d(p^{i\circ}_{pre}, p^i_d) \tag{5}$$

IV. ATTRIBUTE ATTACK GRAPH CONSTRUCTION BASED ON ALARM ASSOCIATION AND STATE SPACE REDUCTION

Based on the above observation, this paper proposes that the edge computing system attack linkage processing decision model, which is shown in Figure 3. It is based on the attribute attack graph. It consists of five parts: trigger condition, strategy decision engine, human-machine interface, strategy template library, and strategy execution point.

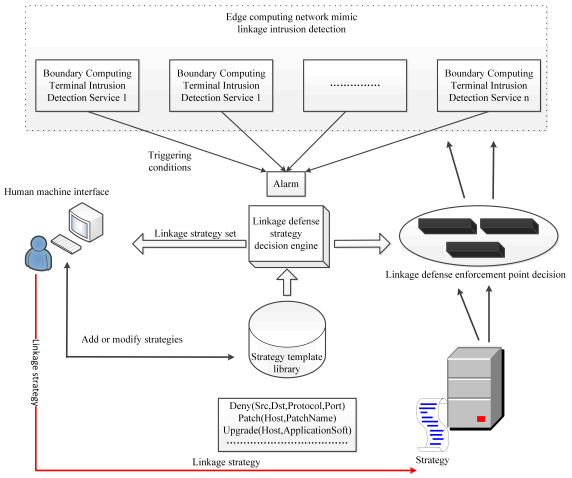


FIGURE 3. Decision-making model of complex attack linkage treatment strategy.

A. NETWORK ATTACK LINKAGE DISPOSITION DECISION MODEL

Among them, the triggering condition mainly includes the linkage intrusion detection alarm information generated by the edge computing terminal intrusion detection service [36], [37]. However, the edge computing network also involves real-time alarms of the intrusion detection device, vulnerabilities in the scanner output, and threat information provided by the network security official organization or website [8], [38]. It is an important part of the active defense of this paper to implement reasonable and optimized security management measures for each type of attack alarm information to improve the system security defense capability. Therefore, the complex attack linkage decision-making model proposed in this paper can also use firewall alarms, IDS alarms, vulnerability information, etc. as strategy trigger conditions. Referring to the alarm classification information in Snort User Manual 2.9.9, the designed linkage strategy decision model covers and includes not only the following alarm types:

- Login attempt for default username and password
- Network scanning
- Denial of service
- Obtain administrator privileges
- Obtain normal user rights
- Trojan activity
- Buffer overflow
- SQL injection
- Path traversal
- Cross-site scripting
- Configuration error
- Information disclosure
- Boundary conditions are wrong
- Format string

The strategy template library is used to store the knowledge of security strategy and is stored by type of trigger condition and provides input to the policy decision engine. The strategy decision engine is the heart of the intelligent decision-making model of the entire linkage strategy. The knowledge in the strategy template library is invoked and instantiated according to the trigger condition. The security linkage strategies and their combinations are further applied to the attack graph and assessing the vulnerability of the corresponding system security. Finally, we get security linkage strategy and its corresponding system security posture value to the security administrator [39], [40].

The human-machine interface has two major functions: i) Responsible for analyzing and confirming the enforceability of the security strategy [41]. The main reason is the impact of the implementation of the linkage strategy on the system security vulnerability and the enforceability of the strategy. ii) Add and modify knowledge in the strategy template library as needed. The strategy enforcement point is responsible for implementing the issued security policy, mainly by modifying the rules of the firewall and the security isolation device [42]–[44].

The decision-making goal of the linkage disposal strategy is reflected in the improvement of the system security defense resistance, that is, the risk of the vulnerability of the edge computing system, i.e., as a whole this can be significantly eliminated [45]. To this end, the paper designs a linkage disposition strategy decision engine based on the attribute attack graph, and takes the security impact of the linkage disposition strategy on the probability of the system's global vulnerability being exploited as the decision basis. The engine uses the alarm information set corresponding to the trigger condition as input and associates the alarm information with the attack source and the destination attribute to determine an attack coverage asset node object, that is, the atomic attack node of the attribute attack graph. At the same time, taking the current security configuration information, vulnerability information and vulnerability utilization policy information as input, the causal relationship of the alarm information is determined, thereby constructing an attribute attack graph. The attribute attack graph state space is further reduced based on the redundancy decision algorithm. Under the assumption of the action set of the linkage disposition strategy, the linkage disposition strategy is determined based on the minimum dominance set and the game return equilibrium condition. The linkage disposition strategy decision engine model is shown in Figure 4.

B. ATTRIBUTE ATTACK GRAPH CONSTRUCTION BASED ON ALARM ASSOCIATION

Currently, the generation of attribute attack graphs is mainly based on the method of reasoning. The principle of attribute attack graph generation based on reasoning is to first define network topology information, inter-host connection information, vulnerability information, and security rules according to certain specifications, and describe atomic attacks with formal rules, then use logical reasoning tools to infer the entire attack scene to find all attack paths [46]. Currently used inference tools mainly include attack graph generation tool MulVAL. In this paper, the edge computing network attack linkage processing decision algorithm based on the attribute attack graph is proposed. Firstly, the atomic attack nodes involved in the network attack event are obtained through the association of alarm attributes. Secondly, the MulVAL-based inference algorithm is used to determine the attack-related attribute nodes. Therefore, the attribute attack graph for the alarm defense is constructed efficiently. At the same time, considering the existence of a large number of redundant alarms in the alarm information, the attribute attack graph faces the problem of space explosion. In this section, a redundant alarm determination method based on K-means clustering is proposed to effectively reduce the state space of the attribute attack graph.

1) ATOMIC ATTACK NODE DETERMINATION

According to the definition of the attribute attack graph, based on the attribute attack graph construction of the alarm association, determining the atomic attack node becomes the first step. For the network attack alarm information generated in a specific network, the atomic attack node connection graph $G_{atom} = (V_{atom}, E_{atom})$ is constructed to represent the relationship between the intrusion source host and the

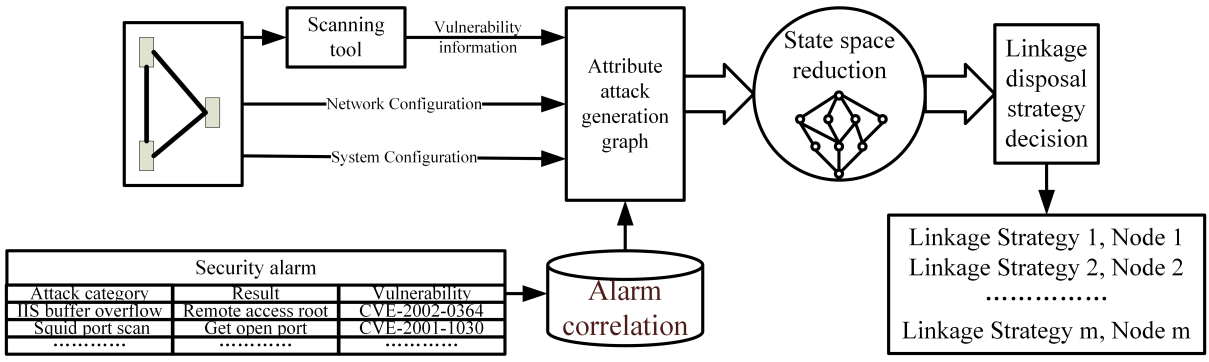


FIGURE 4. The model of linkage disposal strategy decision engine.

victim host, where V_{atom} represents the set of network host nodes involved in the alarm information, and E_{atom} represents the set of inter-host attack events involved in the alert. The host node set V_{atom} contains two kinds of nodes that one is the intrusion source host node, and the other is the victim host node. Suppose the intrusion source host node A invades the attacked host node C by a certain attack means, and there is an edge in the edge set E, and v^a_{atom} points to v^c_{atom}.

As shown in Figure 5, the white hollow dot is the host node for the attack target, and the black solid dot is the host node of the intrusion source. The larger white hollow dots in the middle gather scattered edges connecting different nodes, indicating that multiple intrusion source host nodes invade the target host node through the network attack. There are many densely concentrated boundaries at the bottom of the figure, and one end of these edges originates from the same host node, indicating that there are multiple network security alarms between the host node and the terminal node.

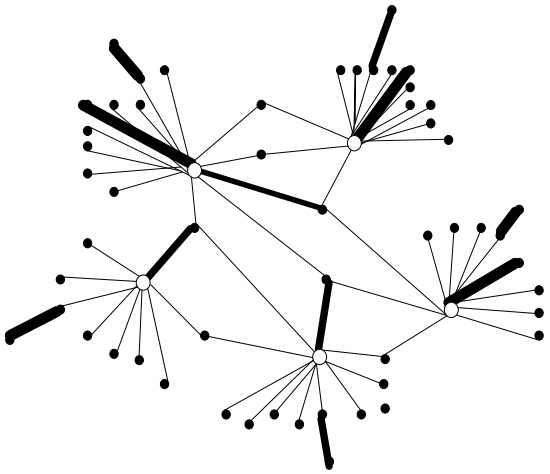


FIGURE 5. Schematic diagram of alarm correlation.

Assume that the connection diagram of the atomic attack node is constructed as $G_{atom} = (V_{atom}, E_{atom})$, $V_{atom} = \{v^1_{atom}, v^2_{atom}, L, v^n_{atom}\}$, the adjacency matrix is defined as:

$$Ac = \begin{bmatrix} ac_{11} & \cdots & ac_{1n} \\ \vdots & \ddots & \vdots \\ ac_{n1} & \cdots & ac_{nn} \end{bmatrix} \tag{6}$$

The number of edges between nodes in E_{atom} is also the number of alarm events. If there are n edges in v^i_{atom} to v^j_{atom}, then $ac_{ij} = n$.

2) ATTRIBUTE ATTACK GRAPH GENERATION

Figure 6 shows the connection between the atomic attack node and the attribute node in the alarm event log for a period of time. The black circle indicates the attribute node, and the white circle indicates the atomic attack node. The thickness of the black line between the connected atomic node and the attribute node indicates the frequency of the associated alarm event. The thicker the black line denotes that the more times the attack event alarm is generated.

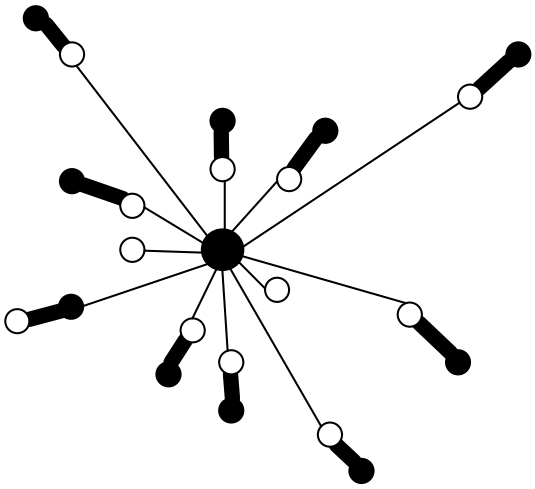


FIGURE 6. Schematic diagram of the node attribute determination of the attribute attack graph.

Based on the above analysis, this section gives the following edge calculation network attribute attack graph generation algorithm based on alarm correlation:

Step 1: input V_{atom} set, E_{atom} set, vulnerable point set $Vulf$, and attack hazard set $Attack$.

Step 2: Add V_{atom} to the initial node status queue, marked as ''not traversed''.

Step 3: If the state queue still has a state node v_i that is not traversed, find the state node v_i that is not traversed. Obtain the corresponding tuple of the attack source node set V_i^{source} and the victim host node-set V_i^{attack} from them E_{atom}. Then the state node v_i is marked as ''self-traversed'' and proceeds to the next step. Otherwise, step (7) is directly performed.

Step 4: For the V_i^{attack} set, if there is a host node that is not traversed, the outbound edge corresponding to the v_i node in E_{atom}, that is, the event hazard from the v_i-initiated attack is marked as the consequence attribute node V_i^{post}. At the same time, the vulnerability list $Vulf_i$ of the host node v_i is obtained. The MulVAL-based inference algorithm determines the vulnerability list of the nodes used to cause V_i^{post}. And record the host node as the initial attribute node V_i^{pre}. Then add an attribute node set V_i^{post} between v_i and V_i^{attack}. Construct a new edge set of $v_i \rightarrow V_i^{post} \rightarrow V_i^{attack}$. At the same time, construct the new premise attribute edge set off $V_i^{pre} \rightarrow v_i$, and proceed to the next step. Otherwise, repeat step (3).

Step 5: For the V_i^{source} set, if there is a host node that is not traversed, then match inbound edge corresponding to a node v_i in E_{atom}, that is, the harm of the event that A is attacked, to the initial attribute node V_i^{pre} traversed in the previous step. If there is the same node, the corresponding attack event in V_i^{source} causes the corresponding initial attribute node in V_i^{pre}. Then delete the corresponding initial attribute node in V_i^{pre}, delete the corresponding edge $V_i^{pre} \rightarrow v_i$, and proceed to the next step.

Step 6: Establish a complete attribute attack graph based on the causal logical reasoning of the attack event.

3) DEGREE CALCULATION OF NODES

In the attribute attack graph, the degree of the node indicates how active a node is. Taking the host node as an example, the degree of the node indicates the number of alarm events that the host is attacked or launched. The outbound degree of a node indicates the number of alarm events that the node is used to implement the attack. The ingress degree of a node indicates the number of alarms generated by the attack that the node is subjected to, and the degree of the node is calculated as follows:

The outbound degree of the node v_i is:

$$d_i = \sum_{j=1}^{n} ac_{ij} \tag{7}$$

The ingress degree of the node is:

$$d_i^{'} = \sum_{j=1}^{n} ac_{ji} \tag{8}$$

According to the above explanation, in the actual situation that there are many redundant alarms in the network, another defect of the generated attribute attack graph is that the monotonic hypothesis is not utilized, and it is easy to cause more attack paths and wrong attack paths in the attack graph, which makes the number of nodes large, and also causes the state space explosion problem in the attribute attack graph generation process.

C. ATTRIBUTE ATTACK GRAPH BASED ON REDUNDANT ALARM CLUSTERING

According to the attribute attack graph construction method proposed in Section 3, this paper firstly determines the atomic attack node by the source and destination host of the network attack alarm event and builds the set E_{atom} based on the set of alarm events between the atomic attack nodes. However, in the event network attack and defense confrontation, multiple security alarms may be generated for the same security device or different security devices at the events from the same source or destination network. This makes the scale of the alarm in the real network environment extremely large, which also causes the problem of the attribute attack graph construction method to explode in the state space. There are a lot of redundant edges in the set E_{atom}.

In response to the above problems, it is necessary to identify and reduce the number of redundant alarms in the edge computing network as much as possible. To this end, this section uses the k-means clustering method to cluster the alarm event set to obtain several alarm event subcategories. For the subsequent decision strategy generation, each cluster subclass is compressed and merged to reduce the redundant edge of the attribute attack graph. The overall process flow framework is shown in Figure 7.

Since we need to examine the distance between each alarm event during the clustering process, we first need to vectorize the alarm events. For a typical network security event alarm log, the information fields usually include the generated

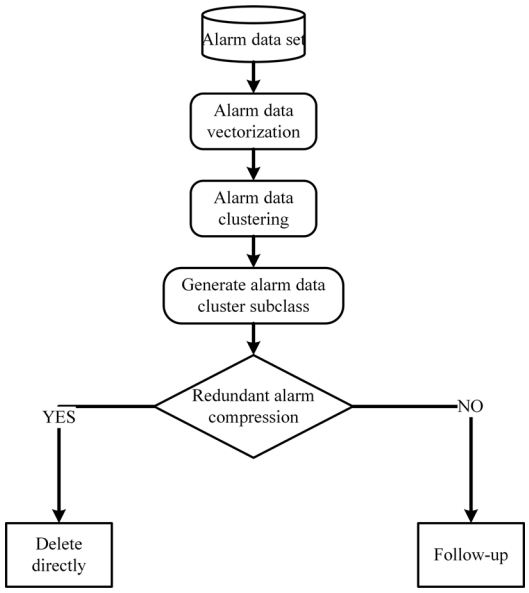


FIGURE 7. The overall process of the redundant alarm processing.

alarm time, the signature ID, the alarm priority, the protocol, the source IP address, the source port, the destination IP address, and the destination port. Because there are many information fields involved, and the alarm formats of different devices and different manufacturers are not consistent, the advanced log formats of various devices are described as follows.

For the field of alarm priority, alarm time, etc., which can express its own degree or trend, you can directly use its original value information as the feature vector. For a field that does not have its own size, such as attack type, source IP, and destination IP, you can classify and then vectorize the attributes of the field. Taking the attack type as an example, we classify according to the possible attack scenarios, and sort according to the degree of harm, and for IP, divide the vector according to the IP address range. In summary, the goal is to convert the original alarm event record into a vector form that can be calculated. The conversion process is shown in Figure 8.

In order to effectively classify the original alarm events, the K-means clustering method is first used to cluster the original alarm event sets. Cluster analysis is a process of dividing a large data set into multiple subsets. Each subclass obtained by clustering is similar to each other, but the subclasses are different from each other. The processing flow of the K-means algorithm is to randomly select k objects in the original alarm event data set as the center of a cluster. Then, for all remaining alarm events, calculate the distance from other alarm events to the cluster center, and divide each alarm event into the cluster class closest to it according to the obtained distance. Then, the K-means algorithm iteratively improves intra-cluster errors. For each cluster, use all alarm events in the cluster to calculate a new mean, then use the new mean like the new cluster center, and reassign all objects to

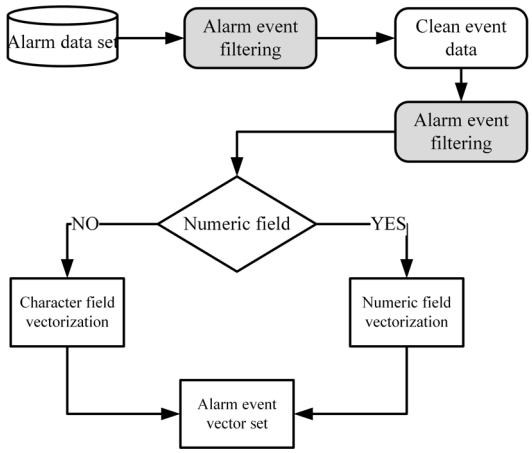


FIGURE 8. Vectorization of alarm events.

the new closest cluster class. Iterate until the error within the cluster class is less than a given value or no longer changes. The specific clustering process is shown in Figure 9.

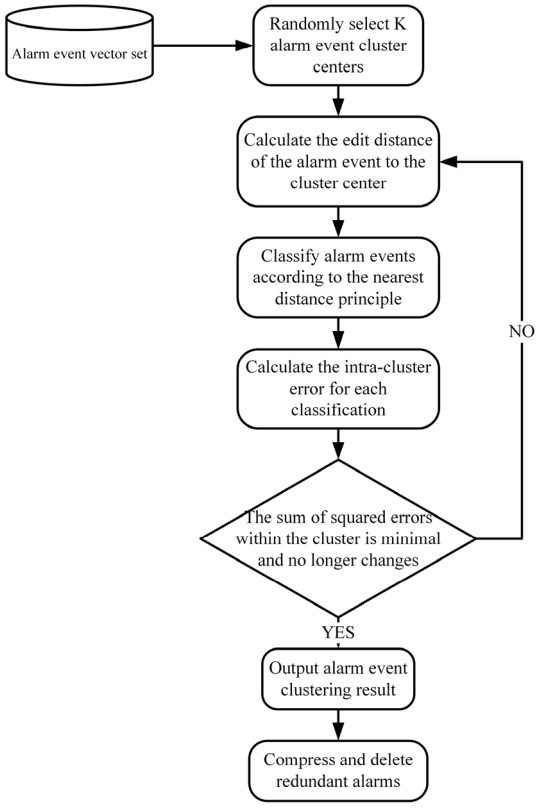


FIGURE 9. Alarm event clustering process.

V. OPTIMAL LINKAGE DISPOSITION STRATEGY DECISION ALGORITHM IN EDGE COMPUTING NETWORKS

After completing the attribute attack graph construction, which is based on the alarm association, the state space reduction and the redundant alarm determination, this section proposes an algorithm for calculating the optimal linkage processing, as shown in Algorithm 1. First, all the nodes in the figure are identified and classified into the initial attribute node set, the atomic attack node set, and the consequence attribute node set according to the out-degree and in-degree obtained by the FIND-STRATEGY algorithm in Algorithm 1. On this basis, through the GREEDY-SET-COVER algorithm shown in Algorithm 2, find a set which covers all atomic attack nodes of the attack graph AG and has the minimum number of initial attribute nodes, which is the final required MDS set. Finally, the attack and defense income calculation is performed for each subset of the MDS set, and the optimal defense strategy is solved by Nash equilibrium conditions.

For the attribute attack graph $AG = (V, E)$ with "m" atomic attack nodes and "n" initial attribute nodes, the time complexity of the GREEDY-SET-COVER algorithm used in this paper is O (mm). In general, the collection coverage problem is an optimization problem.

Algorithm 1 Find-Strategy Algorithm

Input: $AG = (V, E)$
Output: $(p^{i\circ}_{pre}, p^{i\circ}_{d})$
1: **Start**
2: $\langle V, E\rangle \leftarrow MST\ (AG)$
// Identify all nodes and edges in an AG using the minimum spanning tree algorithm
3: **for** all $v \in V$ do
4: **if** $(id(v) = 0 \wedge od(v) \geq 1)$
5: Mark node v as the initial attribute node
6: **else if** $(id(u) \geq 1 \wedge od(u) = 1)$
7: Mark node v as the consequence attribute node
8: **else**
9: *PostCondan*
10: **end if**
11: **end for**
12: **for** all $v \in$ Initial attribute node set do
13: $c_i \leftarrow o(v)$
14: **end for**
15: Calculated dominating set $C = V^{n}_{i=1} c_i$; where $n =$ |Initial attribute node|
16: MDS(AG)←GREEDY-SET-COVER(Exploit, C)
17: **for** all $mds \in MDS(AG)$
18: Calculate pt^{i}_{pre}, pt^{i}_{d}
19: Solve $(p^{i\circ}_{pre}, p^{i\circ}_{d})$
20: **end for**
21: Output $(p^{\circ}_{pre}, p^{\circ}_{d})$
22: **end**

VI. EXPERIMENT AND ANALYSIS

A. EXPERIMENTAL ENVIRONMENT SETTINGS

This section performs the analysis using the network environment shown in Figure 10. *Host*3 is the attacker's target host, and the Mysql database service running on it is a key resource. The attacker is a malicious entity whose goal is to gain root

Algorithm 2 Greedy-Set-Cover Algorithm

Input: Collection cluster $S(i) = S_i(1 \leq i \leq n)$ **is a subset of the atomic attack node set** ε

Output: Coverage set D

1: **Start**
2: $U \leftarrow \varepsilon$
3: $D \leftarrow \emptyset$
4: **while** $U \neq \emptyset do$
5: Select $S(j) \in S$ that maximizes $|S(j) \cap U|$ where $j \leq n$
6: $U - S(j)$
7: $D = D \cup S(j)$
8: $S(i) = S(i) - S(j), 1 \leq i \leq n$
9: **end while**
10: return D
11: **end**

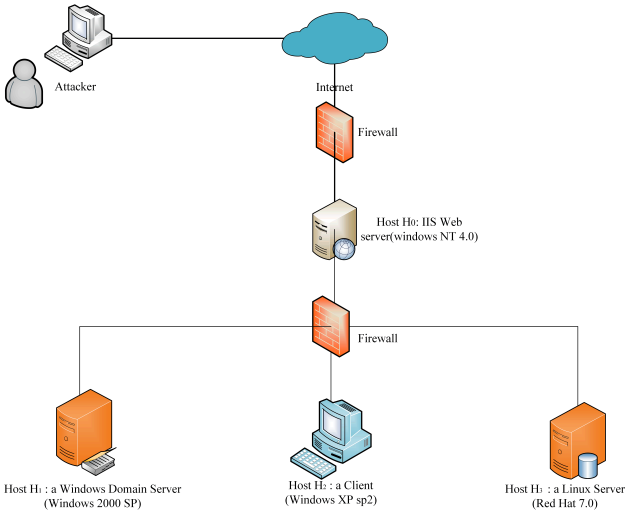


FIGURE 10. Experimental environment settings.

privileges of *Host*3. The firewall separates the target network from the internet. The firewall configuration in the network topology is shown in Table 2.

TABLE 2. Network firewall access control pules.

Host	Attacker	Host0	Host1	Host2	Host3
Attacker	Local-host	All	NONE	NONE	NONE
Host0	ALL	Local-host	ALL	ALL	Squid LICQ
Host1	ALL	IIS	Local-host	ALL	Squid LICQ

Table 3 shows the details of the utilization information of the vulnerable points on each host node in the network. Among them, the information of the vulnerability is from the NVD database. The external network firewall in the network only allows hosts on the external network to access services on Host 0. Connections to any other host will be blocked.

TABLE 3. Utilization information of the vulnerable points.

Host	Services	Ports	Vulnerabilities	CVE IDs
$Host_0$	IIS web service	80	IIS buffer overflow	CVE-2010-2370
	ftp	21	ftp buffer overflow	CVE-2009-3023
	ftp	21	ftp rhost overwrite	CVE-2008-1396
$Host_1$	ssh	22	ssh buffer overflow	CVE-2002-1359
	rsh	514	rsh login	CVE-1999-0180
$Host_2$	netbios-ssn	139	Netbios-ssnnullsession	CVE-2003-0661
	rsh	514	rsh login	CVE-1999-0180
$Host_3$	LICQ	5190	LICQ-remote-to-user	CVE-2001-0439
	Squid proxy	80	squid-port-scan	CVE-2001-1030

The intranet host only allows communication according to the access control rules in Table 2. ALL means that the source host can access all services on the destination host. NONE means that the source host will be blocked from accessing any service of the destination host

B. ANALYSIS OF EXPERIMENTAL RESULTS

1) ANALYSIS OF REDUNDANT ALARM CLUSTERING RESULTS

In order to verify the effectiveness of the redundant alarm clustering compression method proposed in this paper, the alarm log data of Fujian Electric Power Company is used for analysis. The log size is 26.8M and contains 469,010 records. The log format of this type is shown in Table 4.

TABLE 4. Alarm log format.

Serial Number	Field Name	description
0	Timestamp	Alarm time
1	Description	Consisting of Description ID and Description.
2	Classification	Alarm classification
3	Priority	Priority (threat level)
4	Protocol	Traffic protocol
5	Source	Source IP address: source port
6	Destination	Destination IP address: destination port

The K-means clustering method is used to cluster the alarm data. The difference between different attributes may be very large, and they may be measured by different units. In order to eliminate the influence of the metric on the distance, take 8 features for each record in the alarm log: Timestamp, Description ID, Priority, Protocol, SrcIP, SrcPort, DstIP, DstPort, then vectorize and standardize the records. The result of partial data being vectorized is shown in Table 5.

We utilized the K-means method for clustering on the digitized and normalized feature set. Moreover, we reduced and visualized the clustering results using the t-SNE method [47],

TABLE 5. The result of partial alarm data being vectorized.

Timestamp	Description ID	Priority	Protocol	SrcIP	SrcPort	DstIP	DstPort
0.359010526933	-0.189521169276	0.524242583145	-0.534227503613	0.745698068846	0.122249984606	0.829006369326	-0.326140826775
0.359011653393	-0.189677026864	-0.731631428097	-0.534227503613	0.745698068846	0.123096115672	0.829006369326	-0.326140826775
0.359011653393	-0.189521169276	0.524242583145	-0.534227503613	0.745698068846	0.123096115672	0.829006369326	-0.326140826775
0.770163790145	-0.189878707377	0.524242583145	-0.534227503613	0.74046766481	0.123942246738	0.849459889487	-0.326140826775
0.770164259955	-0.189878707377	0.524242583145	-0.534227503613	0.74046766481	0.123942246738	0.849459889487	-0.326140826775
-0.0221354151738	-0.189793075163	-0.731631428097	-0.534227503613	0.735835021235	0.120980788008	0.780249264871	-0.326140826775
0.349078366236	-0.190275557771	-0.731631428097	-0.534227503613	0.735237260773	0.130711295262	0.850745008468	-0.326140826775

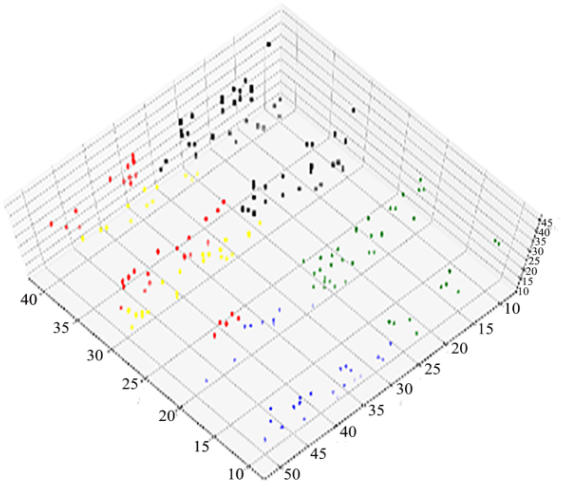


FIGURE 11. Alarm data clustering results.

which is currently the best data reduction and visualization method. Figure 11 shows that the clustering effect is efficient after dimension reduction.

By performing k-means clustering, the relevant alarm information is gathered into the same cluster subclass, and the useless redundant alarm records are also grouped together. On this basis, we compress and merge the alarm cluster subclasses. According to the experimental verification of the traffic data of Fujian Electric Power Company in Figure 12 and Figure 13, the overall redundant alarm compression rate can reach more than 97.2%.

2) ANALYSIS OF THE RESULTS OF LINKAGE EXECUTION OPTIMAL EXECUTION POINT DECISION

The attribute attack map generated according to the network topology as shown in Figure10 and the access control rules as shown in the table is as shown in Figure 14. The atomic attack nodes are represented by ellipses, the initial attribute nodes are represented by rectangles, and the consequence attribute nodes are represented by plain text. The premise attribute node and the consequence attribute node are connected elliptically between each atomic attack. From Figure 14, there are a total of 17 atomic attack nodes in the figure. If an atomic attack is to be successfully implemented, its premise attribute nodes must all be satisfied. The consequence attribute node cannot be removed unless the actual cause (such as vulnerability, unnecessary service/open port) that caused it has been removed from the network. On the other hand, the initial

Security device alarm of State Grid Fujian branch

There are 16, 782 records in this time period, matching 2541 records, showing 1000 records, and the total time is 0 seconds.

30 records per page

Serial number	Starting time	End time	Host MAC	Event type	Number of aggregation events
1	10/12/19:11:35	10/12/19:13:13	fc:4d:d4:d9:f4:51	malicious software(Virus. Win32.Sality.I)	9
2	10/12/19:11:35	10/12/19:13:13	fc:4d:d4:d9:f4:51	malicious software(Virus. Win32.Sality.I)	9
3	10/12/19:11:35	10/12/19:13:13	fc:4d:d4:d9:f4:51	malicious software(Virus. Win32.Sality.I)	9
4	10/12/19:16:09	10/12/19:25:31	f8:b1:56:9f:79:fa	malicious software(Virus. Win32.Sality.I)	40
5	10/12/19:16:09	10/12/19:25:31	f8:b1:56:9f:79:fa	malicious software(Virus. Win32.Sality.I)	40
6	10/12/19:16:09	10/12/19:25:31	f8:b1:56:9f:79:fa	malicious software(Virus. Win32.Sality.I)	40
7	10/12/21:34:46	10/12/21:34:46	fc:4d:d4:f7:99:ad	malicious software(virus.ini.startpage.a)	1
8	10/12/21:34:46	10/12/21:34:46	fc:4d:d4:f7:99:ad	malicious software(virus.ini.startpage.a)	1
9	10/12/21:34:46	10/12/21:34:46	fc:4d:d4:f7:99:ad	malicious software(virus.ini.startpage.a)	1
10	10/12/23:03:20	10/12/23:03:20	b8:ca:3a:93:ff:1b	malicious software(Virus. Win32.Sality.I)	1
11	10/12/23:03:20	10/12/23:03:20	b8:ca:3a:93:ff:1b	malicious software(Virus. Win32.Sality.I)	1
12	10/12/23:03:20	10/12/23:03:20	b8:ca:3a:93:ff:1b	malicious software(Virus. Win32.Sality.I)	1

FIGURE 12. Alarm data aggregation compression result (a).

Serial number	Time	Source IP	Destination IP	Destination port	Event type	Number of aggregation events
1	07/01/00:06:38	192.168.31.10	37.157.255.28	80	A Network Trojan was Detected	25
2	07/01/00:06:52	192.168.31.10	213.108.252.185	80	A Network Trojan was Detected	8
3	07/01/00:07:25	62.76.47.61	192.168.31.10		Misc activity	4
4	07/01/00:07:44	178.162.167.135	192.168.31.10	1040	Potential Corporate Privacy Violation	1
5	07/01/00:07:44	178.162.167.135	192.168.31.10	1040	Misc activity	2
6	07/01/00:07:46	78.140.131.158	192.168.31.10	1076	Web Application Attack	1
7	07/01/00:08:22	178.162.167.135	192.168.31.10	1041	Attempted User Privilege Gain	3
8	07/01/00:08:22	192.168.31.10	178.162.167.135	80	A Network Trojan was Detected	17
9	07/01/00:09:09	192.168.31.10	239.255.255.250	1900	Detection of a Network Scan	3
10	07/01/00:09:42	192.168.31.10	192.166.218.218	80	A Network Trojan was Detected	1
11	07/01/00:11:24	192.168.31.10	116.255.235.9	80	A Network Trojan was Detected	1
12	07/01/00:13:59	178.162.167.135	192.168.31.10	1040	Attempted User Privilege Gain	1
13	07/01/00:13:59	178.162.167.135	192.168.31.10	1040	A Network Trojan was Detected	3
14	07/01/00:14:55	192.168.31.10	208.91.207.10	80	Potential Corporate Privacy Violation	1

FIGURE 13. Alarm data aggregation compression result (b).

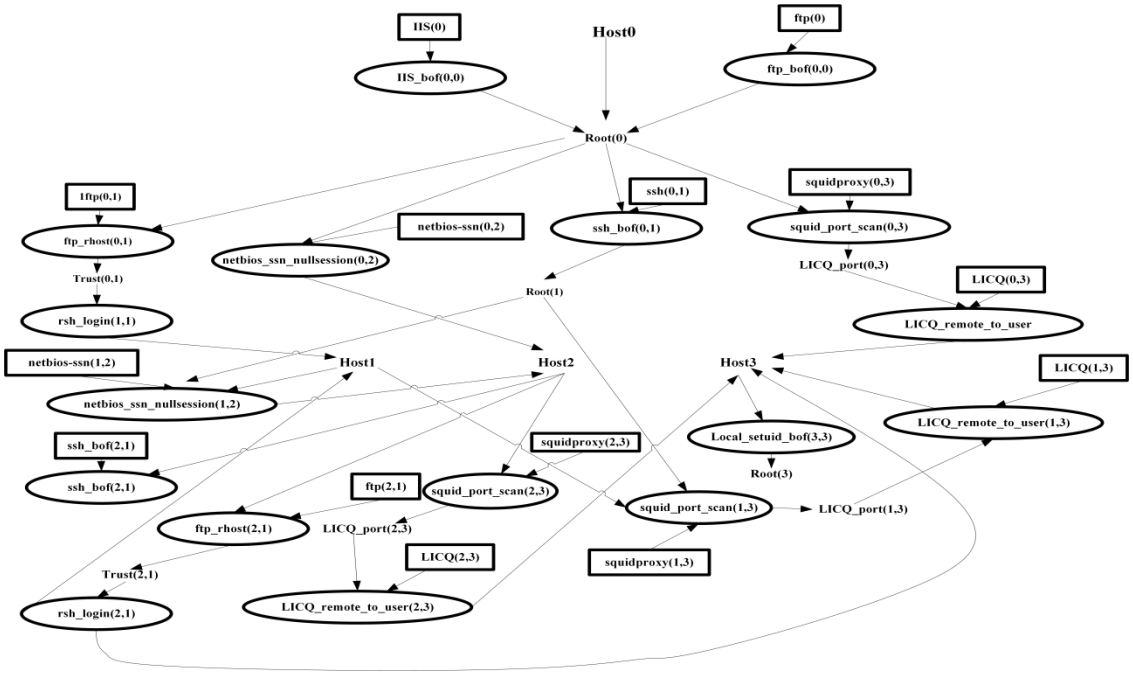


FIGURE 14. Generated attribute attack graph.

attribute node can be removed independently when the linkage decision is made.

By solving the minimum dominance set, the minimum dominance set produced by the above attribute attack graph is:

$$\begin{aligned} MDS = \{&Host0, IIS(0), ftp(0), ftp(0,1), ssh(0,1),\\ &squid-proxy(0,3), net-bios-ssn(0,2),\\ &LICQ(0,3), LICQ(0,3), squid-proxy(1,3),\\ &netbios-ssn(1,2), ftp(2,1), ssh(2,1),\\ &squid-proxy(2,3), LICQ(2,3)\} \end{aligned}$$

Prioritizing the destruction of one or more initial attribute nodes prevents network attacks that require them as a prerequisite, thereby preventing critical resources from being compromised. It is worth noting that the security administrator must consider the cost of these initial conditions when making decisions.

3) ANALYSIS OF THE EFFECTIVENESS OF LINKAGE DISPOSAL STRATEGY

To demonstrate the effectiveness of the proposed method in defense, we analyze the proposed method based on two aspects including, the intrusion success probability and the intrusion time test. Figure 15 shows the comparison results of the success rate of the intrusion edge computing network using the proposed method, the Bayesian network method and game method as the intrusion time increases.

Figure 15 shows that with the gradual increase of time, the successful intrusion rate of the edge computing network is

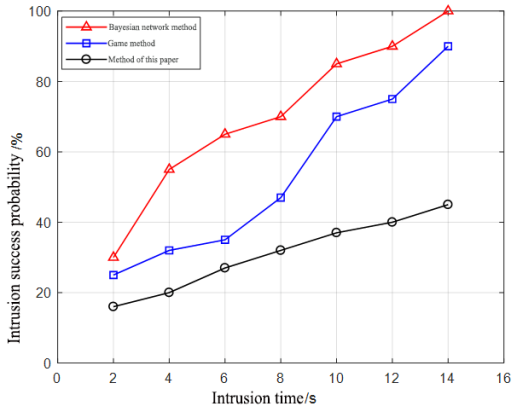


FIGURE 15. Comparison of the probability of successful invasion of three methods.

gradually increased after adopting three methods. However, the successful intrusion rate curve of the edge computing network after using this method is significantly lower than the other two methods, and it is always lower than the Bayesian network method and the game method, which indicates that the method can effectively prevent the intrusion behavior.

Figure 16 shows the comparison results of the successful intrusion rate of the edge computing network using the proposed method, the Bayesian network method and game method as the intrusion rate increases. It depicts that with the gradual increase of the intrusion rate, the successful intrusion rate of the edge computing network is gradually increased after using the three methods. But the intrusion success rate curve of this method is the smallest, which is significantly lower than the Bayesian network method and the game method. .It shows that the method can still maintain a high defense capability when the intrusion rate is gradually increased and the number of intrusion behaviors is gradually increasing.

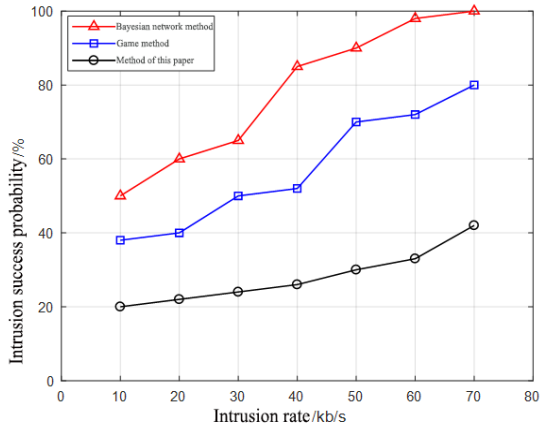


FIGURE 16. Comparison of the success rates of the three methods when the intrusion rate is different.

The significance of the intrusion time test is that the shorter the intrusion time, the more effective the generated attack and defense map is when the intruder invades the edge computing network. Figure 17 depicts the variation of the intrusion time with system time after using the proposed method, Bayesian method and game method.

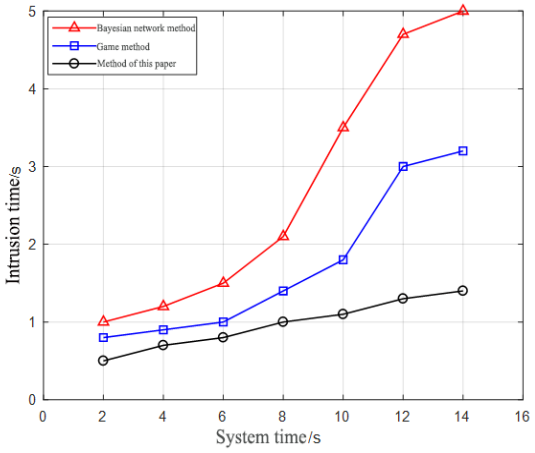


FIGURE 17. The variation of the intrusion time with system time after using three methods.

Figure 17 shows that, after using this method, the edge computing network is invaded for the shortest time, which is significantly lower than the Bayesian network method and game method. It shows that the method is the most difficult to break and the best defensive performance.

VII. CONCLUSION

To realize the rapid response and linkage processing of massive attack events in the edge computing network system environment, this paper studies the complex attack linkage decision-making method in edge computing networks based on the attribute attack graph dominating set theory. Firstly, the linkage processing model of the edge computing network system based on the attribute attack graph is proposed. The attribute attack graph corresponding to the target network is established through the alarm association. The problem is transformed into solving the initial attribute node set minimum dominance set (MDS) to calculate the minimum network defense execution point set. The proposed method can realize the whole network linkage processing based on the minimum-scale node defense and can analyze the best security defense target. At the same time, for the problem of attribute attack graph space explosion caused by redundant alarm, this paper proposes a redundant alarm handling method based on k-means clustering, which reduces the access space of the attribute attack graph node. Finally, the simulation results confirm that the linkage decision algorithm based on attribute attack graph can perform targeted defense on the initial attribute nodes. Thus, it provides the minimum cost defense scheme for complex attacks, and gives a basis for security management personnel to evaluate and control the network security risks. Network security administrators only need to pay attention to a small part of the initial

set of attribute nodes to achieve efficient linkage handling of network attacks. The method in this paper is also applicable to the calculation of network attack linkage disposition decisions of other interconnected systems.

REFERENCES

[1] S. Zhangm, X. Li, Z. Tan, T. Peng, and G. Wang, "A caching and spatial *K*-anonymity driven privacy enhancement scheme in continuous location-based services," *Future Gener. Comput. Syst.*, vol. 94, pp. 40–50, May 2018, doi: 10.1016/j.future.2018.10.053.

[2] L. Qi, X. Zhang, W. Dou, C. Hu, C. Yang, and J. Chen, "A two-stage locality-sensitive hashing based approach for privacy-preserving mobile service recommendation in cross-platform edge environment," *Future Gener. Comput. Syst.*, vol. 88, pp. 636–643, Nov. 2018.

[3] S. Zhang, K.-K. R. Choo, Q. Liu, and G. Wang, "Enhancing privacy through uniform grid and caching in location-based services," *Future Gener. Comput. Syst.*, vol. 86, pp. 881–892, Sep. 2018.

[4] X. Wang, L. T. Yang, X. Chen, M. J. Deen, and J. Jin, "Improved multi-order distributed HOSVD with its incremental computing for smart city services," *IEEE Trans. Sustain. Comput.*, to be published, doi: 10.1109/TSUSC.2018.2881439.

[5] L. Qi, R. Wang, C. Hu, S. Li, Q. He, and X. Xu, "Time-aware distributed service recommendation with privacy-preservation," *Inf. Sci.*, vol. 480, pp. 354–364, Apr. 2018, doi: 10.1016/j.ins.2018.11.030.

[6] X. Wang, W. Wang, L. T. Yang, S. Liao, D. Yin, and M. J. Deen, "A distributed HOSVD method with its incremental computation for big data in cyber-physical-social systems," *IEEE Trans. Computat. Social Syst.*, vol. 5, no. 2, pp. 481–492, Jun. 2018.

[7] K. Peng, V. C. M. Leung, and Q. Huang, "Clustering approach based on mini batch Kmeans for intrusion detection system over big data," *IEEE Access*, vol. 6, pp. 11897–11906, 2018.

[8] S. Zhang, G. Wang, and Q. Liu, "A dual privacy preserving scheme in continuous location-based services," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 4191–4200, Oct. 2018.

[9] X. Xue, Y.-M. Kou, S.-F. Wang, and Z.-Z. Liu, "Computational experiment research on the equalization-oriented service strategy in collaborative manufacturing," *IEEE Trans. Services Comput.*, vol. 11, no. 2, pp. 369–383, Apr. 2018.

[10] Z. Pan, J. Lei, Y. Zhang, and F. L. Wang, "Adaptive fractional-pixel motion estimation skipped algorithm for efficient HEVC motion estimation," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 14, no. 1, Jan. 2018, Art. no. 12.

[11] K. Peng, V. C. M. Leung, L. Zheng, S. Wang, C. Huang, and T. Lin, "Intrusion detection system based on decision tree over big data in fog environment," *Wireless Commun. Mobile Comput.*, Mar. 2018, Art. no. 4680867, doi: 10.1155/2018/4680867.

[12] L. T. Yang *et al.*, "A multi-order distributed HOSVD with its incremental computing for big services in cyber-physical-social systems," *IEEE Trans. Big Data*, to be published, doi: 10.1109/TBDATA.2018.2824303.

[13] C. Hu, A. Alhothaily, A. Alrawais, X. Cheng, C. Sturtivant, and H. Liu, "A secure and verifiable outsourcing scheme for matrix inverse computation," in *Proc. IEEE INFOCOM*, May 2017, pp. 1–9.

[14] X. Wang, L. T. Wang, X. Xie, J. Jin, and M. J. Deen, "A cloud-edge computing framework for cyber-physical-social services," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 80–85, Nov. 2017.

[15] J. Lee, D. Moon, I. Kim, and Y. Lee, "A semantic approach to improving machine readability of a large-scale attack graph," *J. Supercomput.*, pp. 1–18, May 2018.

[16] L. Qi, X. Zhang, W. Dou, and Q. Ni, "A distributed locality-sensitive hashing-based approach for cloud service recommendation from multi-source data," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2616–2624, Nov. 2017.

[17] W. Liu, "APT attack detection and threat assessment based on attack graph," Ph.D. dissertation, Beijing Univ. Posts Telecommun., Beijing, China, 2017.

[18] T. Musa, "Complex network security analysis based on attack graph," *Neuropsychologia*, vol. 12, no. 1, pp. 131–139, 2015.

[19] O. M. Sheyner, "Scenario graphs and attack graphs," Carnegie Mellon Univ., Pittsburgh, PA, USA, 2004.

[20] F. Chen, D. Liu, Y. Zhang, and J. Su, "A scalable approach to analyzing network security using compact attack graphs," *J. Netw.*, vol. 5, no. 5, pp. 543–550, 2010.

[21] S. Roschke, F. Cheng, and C. Meinel, "High-quality attack graph-based IDS correlation," *Log. J. IGPL*, vol. 21, no. 4, pp. 571–591, Aug. 2013.

[22] S. Saurabh and A. S. Sairam, "A more accurate completion condition for attack-graph reconstruction in probabilistic packet marking algorithm," in *Proc. Nat. Conf. Commun. (NCC)*, 2013, pp. 1–5.

[23] M. Alhomidi and M. Reed, "Risk assessment and analysis through population-based attack graph modelling," in *Proc. IEEE World Congr. Internet Secur. (WorldCIS)*, Dec. 2013, pp. 19–24.

[24] P. Yi, A. Iwayemi, and C. Zhou, "Developing ZigBee deployment guideline under WiFi interference for smart grid applications," *IEEE Trans. Smart Grid*, vol. 2, no. 1, pp. 110–120, Mar. 2011.

[25] S. Noel and S. Jajodia, "Metrics suite for network attack graph analytics," in *Proc. 9th Annu. Cyber Inf. Secur. Res. Conf.*, 2014, pp. 5–8.

[26] L. Wang, S. Noel, and S. Jajodia, "Minimum-cost network hardening using attack graphs," *Comput. Commun.*, vol. 29, no. 18, pp. 3812–3824, 2008.

[27] W. Li, *An Approach to Graph-Based Modeling of Network Exploitations*. Starkville, MS, USA: Mississippi State Univ., 2005.

[28] H. Wang, Z. Chen, J. Zhao, X. Di, and D. Liu, "A vulnerability assessment method in industrial Internet of Things based on attack graph and maximum flow," *IEEE Access*, vol. 6, no. 1, pp. 8599–8609, 2018.

[29] F. Chen *et al.*, "Two formal analysis of attack graphs," *J. Softw.*, vol. 21, no. 4, pp. 838–848, 2010.

[30] T. E. Carroll and D. Grosu, "A game theoretic investigation of deception in network security," *Secur. Commun. Netw.*, vol. 4, no. 10, pp. 72–1162, 2011.

[31] F. Wang, J. Xu, X. Wang, and S. Cui, "Joint offloading and computing optimization in wireless powered mobile-edge computing systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1784–1797, Mar. 2018.

[32] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, "OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2274–2282.

[33] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 32, no. 5, pp. 25408–25420, 2017.

[34] R.-H. Hsu, J. Lee, T. Q. S. Quek, and J.-C. Chen, "Reconfigurable security: Edge-computing-based framework for IoT," *IEEE Netw.*, vol. 32, no. 5, pp. 92–99, Sep./Oct. 2018.

[35] R. Pettersen, H. Johansen, and D. Johansen, "Secure edge computing with ARM TrustZone," in *Proc. 2nd Int. Conf. Internet Things, Big Data Secur.*, 2017, pp. 102–109.

[36] L. Deng, H. Zhu, C. Tao, and Y. Wei, "Infrared moving point target detection based on spatial–temporal local contrast filter," *Infr. Phys. Technol.*, vol. 76, pp. 168–173, May 2016.

[37] L. Deng and H. Zhu, "Moving point target detection based on clutter suppression using spatiotemporal local increment coding," *Electron. Lett.*, vol. 51, no. 8, pp. 625–626, Apr. 2015.

[38] A. Rutkin, "Cyberwar becomes official," *New Scientist*, vol. 230, no. 3079, p. 23, 2016.

[39] C. Hu, W. Li, X. Cheng, J. Yu, S. Wang, and R. Bie, "A secure and verifiable access control scheme for big data storage in clouds," *IEEE Trans. Big Data*, vol. 4, no. 3, pp. 341–355, Sep. 2018, doi: 10.1109/TBDATA.2016.2621106.

[40] C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, "Secure and efficient data communication protocol for wireless body area networks," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 2, no. 2, pp. 94–107, Apr./Jun. 2016.

[41] X. Xue, W. Shufang, B. Gui, and H. Zhanwei, "A computational experiment-based evaluation method for context-aware services in complicated environment," *Inf. Sci.*, vol. 373, pp. 269–286, Dec. 2016.

[42] W. Gong, L. Qi, and Y. Xu, "Privacy-aware multidimensional mobile service quality prediction and recommendation in distributed fog environment," *Wireless Commun. Mobile Comput.*, Apr. 2018, Art. no. 3075849.

[43] C. Yan, X. Cui, L. Qi, X. Xu, and X. Zhang, "Privacy-aware data publishing and integration for collaborative service recommendation," *IEEE Access*, vol. 6, pp. 43021–43028, 2018.

[44] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18209–18237, 2018.

[45] Y. Xu, L. Qi, W. Dou, and J. Yu, "Privacy-preserving and scalable service recommendation based on simhash in a distributed cloud environment," *Complexity*, Dec. 2017, Art. no. 3437854.

[46] Y. Zhang and S. Li, "Distributed biased min-consensus with applications to shortest path planning," *IEEE Trans. Autom. Control*, vol. 62, no. 10, pp. 5429–5436, Oct. 2017.

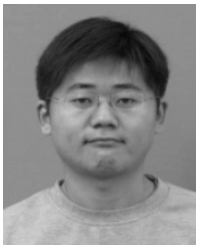
[47] L. van der Maaten and G. E. Hinton, "Visualizing high-dimensional data using t-SNE," *J. Mach. Learn. Res.*, vol. 9, pp. 2579–2605, Nov. 2008.
[48] L. P. Swiler, C. Phillips, D. Ellis, and S. Chakerian, "Computer-attack graph generation tool," in *Proc. 2nd DARPA Inf. Survivability Conf. Expo.*, Jun. 2001, pp. 307–321.

QIANMU LI received the B.Sc. and Ph.D. degrees from the Nanjing University of Science and Technology, China, in 2001 and 2005, respectively, where he is currently a Full Professor with the School of Computer Science and Engineering. His research interests include information security, computing system management, and data mining. He received the China Network and Information Security Outstanding Talent Award, in 2016, and the Education Ministry of Science and Technology Award, in 2012.

SHUNMEI MENG received the Ph.D. degree from the Department of Computer Science and Technology, Nanjing University, China, in 2016. She is currently an Assistant Professor with the School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing, China. She has published papers in international journals and international conferences, such as TPDS, ICWS, and ICSOC. Her research interests include recommender systems, service computing, and cloud computing.

SAINAN ZHANG is currently a student at the Nanjing University of Science and Technology, China. She will graduate from the Nanjing University of Science and Technology, in 2019. Her main research direction is industrial control network security.

JUN HOU received the Ph.D. degree in computer science from the Nanjing University of Science and Technology, China, in 2019, where she is currently an Assistant Professor with the Zijin College. She has published dozens of articles in prestigious journals and top-tier conferences. Her research interests include data mining and information security. She serves as a PC Member for several international conferences and as an External Reviewer for many journals.



LIANYONG QI received the Ph.D. degree from the Department of Computer Science and Technology, Nanjing University, China, in 2011. In 2010, he visited the Department of Information and Communication Technology, Swinburne University of Technology. He is currently an Associate Professor with the School of Information Science and Engineering, Qufu Normal University, China. He has already published more than 30 papers, including JSAC, TCC, TBD, JCSS, FGCS, and CCPE. His research interests include recommender systems and services computing.