Research Article

Research on Multi-Target Network Security Assessment with Attack Graph Expert System Model

Yunpeng Li and Xi Li

Qingdao Vocational and Technical College of Hotel Management, Qingdao, Shan Dong 266100, China

Correspondence should be addressed to Yunpeng Li; liyunpeng@qchm.edu.cn

Received 31 March 2021; Revised 20 April 2021; Accepted 29 April 2021; Published 7 May 2021

Academic Editor: Yi-Zhang Jiang

Copyright © 2021 Yunpeng Li and Xi Li. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the rapid development of the Internet, network attacks often occur, and network security is widely concerned. Searching for practical security risk assessment methods is a research hotspot in the field of network security. Network attack graph model is an active detection technology for the attack path. From the perspective of the attacker, it simulated the whole network attack scenario and then presented the dependency among the vulnerabilities in the target network in the way of directed graph. It is an effective tool for analyzing network vulnerability. This paper describes in detail the common methods and tools of network security assessment and analyzes the construction of theoretical model of attack graph, the optimization technology of attack graph, and the research status of qualitative and quantitative analysis technology of attack graph in network security assessment. The attack graph generated in the face of large-scale network is too complex to find the key vulnerability nodes accurately and quickly. Optimizing the attack graph and solving the key attack set can help the security manager better understand the security state of the nodes in the network system, so as to strengthen the security defense ability and guarantee the security of the network system. For all kinds of loop phenomena of directed attribute attack graph, the general method of eliminating loop is given to get an acyclic attack graph. On the basis of acyclic attack graph, an optimization algorithm based on path complexity is proposed, which takes atomic attack distance and atomic weight into consideration, and on the basis of simplified attack graph, minimum-cost security reinforcement is carried out for the network environment. Based on the ant colony algorithm, the adaptive updating principle of changing pheromone and the local searching strategy of the adaptive genetic algorithm are proposed to improve the ant colony algorithm. The experimental results show that compared with the ant colony algorithm, the improved ant colony algorithm can speed up the process of solving the optimal solution. When the number of attack paths is large, the advantages of the improved ant colony algorithm in solving accuracy and late search speed are more obvious, and it is more suitable for large-scale networks.

1. Introduction

With the increasing number of hosts accessing the Internet, coupled with the complexity of various application hardware and software as well as various network protocols, some code loopholes will occur in the stage of design, development, deployment, and maintenance. In a sense, these loopholes will cause the vulnerability of network system. In addition, the network security tools update too slowly, and hackers use the new technology to network environment vulnerabilities to attack. It also makes the network possible to be paralyzed. The outbreak of all kinds of virus events is a wake-up call for

us. With the improvement in the education level of hackers and the convenient network communication and other modern characteristics, there are more and more systematic attacks against valuable information [1–3].

At first, people use network security tools for network defense. Traditional security defense tools include firewall, intrusion detection system, user authentication, and encryption. Firewall through the development of certain access rules to access the request to force inspection only allows the rules of access into the firewall access. Intrusion detection system is another security door behind the firewall. It can monitor the system safely even in the case of fluctuating

network performance and provide real-time protection against internal and external attacks and misoperation. User authentication and encryption, on the one hand, is to ensure the security of data storage and transmission and, on the other hand, is to prevent data leakage.

However, the traditional network security tools mentioned above all start from the security management means and can only passively discover the attack behavior and the existing vulnerabilities after the attack occurs. There is a lag in the security protection, and the defense effect on the discovery of new vulnerabilities and the attack behavior is very small. Attack diagram simulates the whole attack scenario from the attacker's point of view and then presents the dependencies among vulnerabilities in the target network and presents them in a directed graph. According to the attack diagram, the security manager can intuitively observe the vulnerability relationship of each node and select the minimum cost for the security reinforcement of the node that is prone to permission transition. Attack graph is a kind of active network security defense technology, which makes an in-depth analysis of the vulnerability of each host. In the era of frequent network security, attack graph technology has a very good research value [4–7].

The increasing size of the network, the increasing number of security vulnerabilities, and the increasing education of hackers have all made cyberattacks possible. In the game of network security, in order to strengthen the analysis and defense of hacker attack, security defense has gone through many stages of development. At the initial stage, the corresponding attack behavior was matched according to the known attack rules, and then, the vulnerability scanning tool was used to find the vulnerability information on the host computer. However, the method based on rule matching can only find out the single vulnerability information and cannot find out the potential harm caused by the correlation between vulnerabilities. Later, researchers combined network security with statistics and used relevant models to quantify the probability of being attacked. They no longer studied a single category but extended the research target to the whole network system. Then, with the further development of the research, network security researchers have learned that the analysis of network security and other issues should start from multiple dimensions, so a variety of security risk assessment standards and vulnerability analysis methods are proposed. At present, the research hotspot is the security risk assessment method based on the model, which considers the network security from the perspective of the attacker. The model-based research method can show all possible attack paths in the form of graphs and then carry out qualitative or quantitative analysis on the existing security problems, which is convenient for security managers to understand the security of the network environment [8–12]. It is an active network security defense measure. Among all model-based risk assessment studies, the study of attack graph model is the most in-depth. In view of the advantages of attack graph in network security analysis, it has attracted the attention of a large number of researchers, and some difficulties of attack graph have been gradually overcome. However, in the

security analysis based on large-scale network, the large scale of the generated attack graph seriously affects its readability and increases the difficulty in security analysis. Network composite attack modeling is a bit abstract. We analyze the relationship between vulnerabilities in the network from the perspective of attack and draw out the possible attack path of network attack, which can effectively evaluate the direct and indirect security impact caused by network attack. This is to find out the possible attack path, if cooperated with IDS, can be used to predict the attack target. Therefore, now, the study of attack graph automated build technology mainly includes the attack graph and the security analysis of the attack graph. Attack graph automatic construction technology includes target environment modeling technology, vulnerability automatic knowledge base construction technology, attack graph algorithm optimization technology, and attack graph, as shown in Figure 1; the relations between the key technologies of attack graph are as follows. Similarly, the following mainly introduces the research status of attack graph technology from the construction, optimization, and security analysis of attack graph [13–15].

2. Network Security Risk Assessment Based on Attack Graph

2.1. Security Risk Assessment Model. Because network security risk assessment technology plays a positive role in strengthening network defense, researchers have never stopped studying in this field. Initially, researchers had to rely on manual assessments or assistive tools to assess risk. However, manual evaluation is a heavy workload, easy to make mistakes, and has certain subjectivity. Risk assessment tools primarily utilize vulnerability scanning tools. This tool can find information such as server or system environment configuration errors, such as ISS, Nessus, and Nmap. Vulnerability scanning tools mainly use rule matching database to find known vulnerability information. At present, foreign authoritative vulnerability databases include National Vulnerability Database (NVD) of the United States and Bug Trap Vulnerability Database released by Symantec. Authoritative vulnerability databases in China include China National Vulnerability Database (CNNVD). Although the risk assessment tool alleviates the workload of manual assessment to some extent, it can only find known vulnerabilities based on the vulnerability database and cannot find unknown vulnerabilities. Furthermore, only single vulnerabilities can be identified, and neither the correlation between vulnerabilities cannot be found nor the potential harm brought by the correlation between vulnerabilities to the system environment can be evaluated [16–19]. Through RFID, sensing, and other technologies, intelligent bus can understand the location of the bus in real time and realize functions such as turning and route reminder. At the same time, combine with the characteristics of the bus operation, through the intelligent scheduling system, the line, vehicle planning, and scheduling, to achieve intelligent scheduling.

Considering the many defects of manual assessment and auxiliary assessment tools, researchers began to study the relationship between vulnerabilities in system environment

FIGURE 1: Attack graph algorithm optimization technology and attack graph.

by using the security risk assessment method of the model. The model-based security risk assessment method takes the network attack modeling technology as the core, simulates the intrusion scenario of the attacker, and evaluates the network system defense capability qualitatively or quantitatively by means of graph theory. The existing model evaluation methods mainly include fault tree model, attack tree model, privilege graph model, attack graph model, and Bayesian network model. After many years of research on fault tree model, some achievements have been made in determining the deterministic direction of the system. The logical relationship between the fault and the cause of the fault in the fault tree is represented graphically. The logical schematic diagram of the fault tree is shown in Figure 2, where T represents the top event and $S1-S4$ represents the bottom event.

Fault tree is a top-down research method, which analyzes the factors that may cause threats to the network environment and displays all possible failures in the form of graphs. Fault tree can also be called deductive analysis; that is, the analysis starts from the top event (the least expected event) and then from the top of the tree to the leaves of the tree analysis, reverse analysis of the root cause of the top event. The results can be used to analyze how multiple components can cause system failure. The fault tree model includes qualitative analysis and quantitative analysis. Qualitative analysis is to use the fault tree to solve the minimum critical attack set of an event. In quantitative analysis, because the failure rate of a single system event is unknown, only the probability of top event occurrence is calculated [20].

On the basis of fault tree, attack tree targets the inherent threat of the system acquired by different types of attack. Attack tree is also used to describe the whole process of the network system being attacked in a top-down way. The root node in the attack tree represents the attack target, the leaf node represents the attack mode adopted, and the nonleaf node represents the attacked subtarget. The nodes of the

FIGURE 2: The logical schematic diagram of the fault tree.

attack tree fall into two categories: AND nodes and OR nodes. The presentation of AND nodes and OR nodes is shown in Figure 3.

The AND node can only pass the task up when all the child nodes are implemented; the OR node can pass the task up as long as any of the child nodes are implemented.

As proposed in a method for manually building state attack graphs, attack graph model can be regarded as a combination of multiple attack tree models in structure. Attack graph describes the attack behavior of multiple different attack targets and shows the attack path in the way of directed graph. The node and edge in the figure describe the vulnerability or attack behavior of the node, and then according to their logical relationship, the attack path containing the attack starting point, vulnerability node, and attack target is generated. The construction of attack graph model has experienced from manual construction to automatic construction based on model detection and then to the generation of attack graph based on logical reasoning process to adapt to the large-scale network environment,

FIGURE 3: The nodes of the attack tree fall into two categories.

thus solving the problem of generating attack graph due to the exponential growth of network scale. Compared with other models, the attack graph model simulates the real attack scenario and detects the vulnerability nodes in the network from the perspective of the attacker. To make the description of network attack more specific and more reliable, the model is as follows:

$$k = \begin{cases} \arg \max \left\{ g(x, y) \eta^e(x, y) + \sqrt{\frac{n(n-1)(n+1)}{2}} \right\}, r \neq r_0, \\ \sqrt{\frac{n(n-1)(n+1)}{2}}, \text{ others.} \end{cases} \quad (1)$$

Bayesian network is a model that combines probability analysis and graph theory to describe uncertain causality. Firstly, it assigns probability values to the nodes or edges of the attack graph model and then calculates the attack probability from the initial node to the target node according to the whole attack process and carries out integration processing. The integrated probability is used as the reference index of the whole system network security. Figure 4 is a simple Bayesian network with four variables: the four nodes in the figure correspond to the four real events, and the value of each node is discrete and can only be true or false, so the conditional probability distribution of each node can be described in the form of table.

2.2. Network Security Risk Assessment Process Based on Attack Graph. According to the research status, the attack graph model is the most effective model to represent the dependency and causality of vulnerability and plays an important role in network security assessment. Based on the construction, optimization, and analysis of attack graph-based network security risk, assessment flow chart is proposed in this section. As shown in Figure 5, the network security risk assessment process based on attack graph in this paper is divided into three modules, namely, the formal representation module of abstract network environment, the generation and optimization module of attribute attack graph, and the solution module of key attack set based on attack graph. Abstract network environment formal representation module is not only the basis of network security analysis but also the premise of the latter two modules. This module mainly contains the important file configuration information in the system network. This information can be obtained through vulnerability scanning tools and port scanning tools. The main contents of this paper are the optimization of attribute attack graph generated in large-scale networks and the solution of the minimum critical attack set of simplified attack graph.

Attribute attack graph is constructed with mature tools, which have been studied by predecessors, but the attack graph constructed in large-scale network has some problems such as low readability and unsatisfactory guidance for security managers. To solve this problem, the simplified

FIGURE 4: A simple Bayesian network with four variables.

attack graph is an improvement in the low readability of the complex attribute attack graph. The attack graph with complex attributes is simplified by using the optimization algorithm based on attack distance and atomic weight, which deletes the meaningless nodes and paths in the real attack path and enhances the readability of the complex

attack graph. Moreover, in the further simplification, the calculation method of path complexity is defined, and attack graphs of different simplified degrees can be obtained by taking different Min value t , which plays a certain role for security managers to predict and judge network risks. The model is as follows:

$$\Omega_{xy}(m+1) = \sqrt{\frac{n(n-1)(n+1)}{2}} + \prod \omega_{xy}^{ck}(m) + (1 - \bar{\sigma})^{(m+1/m-1)}, \Omega = \Omega_{\max}, \quad (2)$$

$$\Omega_{xy}(m+1) = \sqrt{\frac{n(n-1)(n+1)}{2}} + \prod \omega_{xy}^{ck}(m) + (1 + \bar{\sigma})^{(m+1/m-1)}, \Omega \neq \Omega_{\max}.$$

$$\prod \omega_{xy}^{ck}(m) = \begin{cases} (1 - \bar{\sigma})^{(m+1/m-1)}, & \Omega = \Omega_{\max}, \\ (1 + \bar{\sigma})^{(m+1/m-1)}, & \Omega \neq \Omega_{\max}. \end{cases} \quad (3)$$

After the simplified attack graph is obtained, only the key nodes in the attack graph are used for quantitative analysis and security analysis, and the results are uncertain. In the third module, how to solve the minimum critical attack set is proposed, which provides a reliable analysis basis for the minimum network security reinforcement of the network system. Firstly, it is proved that

solving the minimum critical attack set problem is equivalent to the NP-complete problem. In solving the NP problem, the traditional ant colony algorithm will have the problem of premature convergence and slow search speed in the later period, resulting in only obtaining the local optimal solution. Therefore, this paper proposes an improved ant colony algorithm to solve the

FIGURE 5: The network security risk assessment process based on attack graph.

NP problem. By improving the adaptive update of its pheromone and using the adaptive genetic algorithm to carry out local search, the minimum critical attack set can be solved more accurately and the search speed can be accelerated in the later stage of the algorithm, which provides guidance for the network security management personnel to make the minimum cost network reinforcement measures.

This chapter first introduces several network security risk assessment models and analyzes the advantages and disadvantages of each security risk assessment model in detail. Then, several common attack graph models are introduced, with emphasis on attribute attack graph. On the basis of attribute attack graph, the general formal description and representation of network security elements are given. Finally, this paper describes the security risk assessment flow chart based on the attack graph model and introduces the

function of each module in the flow chart in detail, which lays a foundation for the following research implementation.

3. Analysis and Implementation of Multiobjective Optimization Algorithm of Attack Graph Expert System Model

3.1. Multitarget Attack Graph Construction Technology. Attack diagram correlates the vulnerability among hosts in the network, actively discovers the existing vulnerabilities, and represents the possible attack paths in the way of directed graph, but with the expansion of network scale, the problem of space state explosion exists in the construction of attack graph. Too many redundant attack paths in the attack diagram seriously affect the quantitative analysis and accurate judgment of network security by security analysts, thus increasing the cost of network defense. To solve this

problem, this chapter firstly deals with the elimination of the loop in the attack path of the attack graph. Then, in the analysis of the acyclic attack graph, the definition of the path complexity is given based on the attack distance and the weight of atoms. Using different t values to get different degrees of simplified graph, it can improve the readability of the attack graph, which is the possibility of the attack graph being realized in the quantitative analysis of network vulnerabilities.

There are two types of edges in the attribute attack graph: one is the edge from the state node to the attack node, which represents the requirement relationship; the other is the edge from the attack node to the attribute node, which represents the implementation relationship. Figure 6 is an example of a property attack graph. The ellipse represents the attack node, and the text represents the attribute node. When an attacker invades a target network, he first takes advantage of the vulnerability on a host to obtain the initial permissions, and then, he invades again on this basis and repeatedly until the attacker achieves the final target of his attack. Therefore, the process of the attacker's intrusion is actually a transition process from the premise network state to the result network state. Attack graph and related concepts are defined, and construction techniques are explained in the following paragraphs.

The construction of attribute attack graph in this paper adopts the modeling method based on logical reasoning proposed by OU—MuiVal. This modeling method is built on the basis of Prolog logic system and XSB reasoning engine. MuiVal is also an inference system for automatic identification of network vulnerabilities within enterprises. The modeling idea is to first describe the network configuration information and system security policy in a general form, then select its attack behavior as the inference rule, and finally use the XSB inference engine to judge the security policy, if not, then give all possible attack paths. The time complexity of MuiVal is to generate attack graph. MuiVal is a commonly used attack graph building tool. The design principle of MuiVal is to represent the network system configuration information by means of datalog. Attack behavior and defense measures can also be classified using datalog.

Attribute attack graph has two nodes: attribute and attack, which show attack path implicitly. Therefore, there may be multiple attack nodes repeatedly attacking an attribute node, but there is also a relationship between attack nodes with jumping permissions, so it is easy to cause the phenomenon of attack graph loop. The existence of loop makes the relationship between nodes more complex, which has a serious impact on the accuracy of attack probability calculation and the readability of attack graph. It is found that the loop phenomena of attack graph can be divided into three categories.

As shown in Figure 7, text represents the attribute node and ellipse represents the attack node.

But in the multitarget network, deleting a node in the third type of loop may delete the attack path with high-risk probability. In the further study, it is found that if the forward search or depth-first search method is used to calculate all the reachable parent nodes. In the iteration process, in order to eliminate the ring of attack path, the

trace set was defined to place the tracked attribute node that was searched. Before iteration, place all the child nodes of the attribute node to trace the collection and then iterate the child nodes of the node in attack, and in the process of iteration, if the attribute node of the child node is found to be placed in the track, or the child node is found to have been tracked, then the iteration will continue to enter the loop until the iteration is terminated.

As an intelligent subject, the attacker often chooses the attack path with short attack distance and low attack complexity to attack when carrying out network attack. Based on this fact, there are a lot of redundant attack paths in the attack graph. Therefore, in the optimization process of attack graph, if the path complexity of each attack path is calculated according to the attack distance and atomic weight and then a value is set to remove those lower than these safe paths, the attack graph will be simplified to a large extent. Calculation of path complexity is as follows:

$$R = \begin{cases} \prod \omega_{xy}^{ck}(m), m \triangleq 125, \\ \sqrt{\frac{n(n-1)(n+1)}{2}}, \text{ others.} \end{cases} \quad (4)$$

In order to verify the feasibility of eliminating loops for these three types of loops and the scalability of path complexity, we conducted two experiments. In the first part of the experiment, we use the MuiVal attack graph building tool to generate attack graph for a certain scale network environment, analyze the loop condition of attribute attack graph, give the idea of eliminating the loop, and get the acyclic attack graph. The second part of the experiment is to calculate the path complexity of acyclic attack graph, according to different values can get different scales of simplified attack graph. For different values, if different thresholds are set, the number of paths reserved in the simplified graph can be obtained is different. The result is shown in Figure 8.

It can be concluded from Figure 8 that the number of attack paths reserved under different Min values is also different. As the selection of threshold increases, the number of paths reserved decreases. When the value reaches a certain value, all possible attack paths must be removed. Therefore, the selection of the value is also empirical to a certain extent. If the value is too high, the simplified graph is too simple, and it is easy to delete the important nodes of the original attack graph, resulting in the wrong defense reinforcement of the attack nodes. If the value is selected too low, the simplified graph is still complicated, which makes the visibility of attack graph low and the risk assessment for security managers still very difficult.

4. Attack Diagram Expert System Model Multitarget Network Security Algorithm Evaluation

Genetic algorithm is a random search method imitating the biological evolution process. By sacrificing the limited iteration time to optimize the search speed, the algorithm can

FIGURE 6: An example of a property attack graph.

FIGURE 7: Text represents the attribute node and ellipse represents the attack node.

FIGURE 8: The number of paths reserved in the simplified graph.

automatically obtain and guide the optimal search space and adjust the search process adaptively. Because of its bionic nature, it can provide another way to solve problems that other science and technology cannot or are difficult to solve. It has been widely used in combinatorial optimization, machine learning, artificial intelligence, and other fields. However, the traditional genetic algorithm has strong robustness in solving the global optimal solution, which leads to some characteristics such as premature convergence and slow search in the late period. To solve this problem, an adaptive genetic algorithm was proposed, which made the ant colony self-adjust the crossover rate and mutation rate according to its own race. The optimization problem can be

described by the following mathematical programming model.

Figure 9 describes the variation trend of the fitness of the three algorithms. It can be seen from the figure that the adaptive genetic algorithm maintained a high search speed in the early and middle periods and began to slow down its search speed in the 160–180 generation. In the 30th generation, genetic algorithm and adaptive sorting algorithm began to show a step-down state. In the 60th generation, their search speed was slow, and even in the 20th generation, their search speed was almost stagnant. As can be seen from the above, when different values of t are taken, the simplified graphs obtained are also different, and the minimum critical attack sets obtained through the improved ant colony algorithm are also different. However, the security manager can select the values according to the security management resources he/she has, so as to ensure the minimum security network reinforcement measures.

Figure 10 describes the variation curve of the performance of the adaptive genetic algorithm between the optimal individual value and the population mean value. It can be seen from the figure that the convergence performance of the adaptive genetic algorithm is relatively slow in the 0–80 generation and gradually begins to converge to complete the solution of the optimal solution after the 80 generation.

FIGURE 9: The variation trend of the fitness of the three algorithms.

FIGURE 10: The variation curve of the performance of the adaptive genetic algorithm.

It can be seen from Figure 11 that, under the same threshold value t , the minimum critical attack set can be solved for attack graphs of different scales. It can be seen that the improved ant colony algorithm can solve the key attack set more optimally. In addition, it can be seen from the figure that, in the case of increasing attack paths in the attack graph, the optimal solution effect of the improved ant colony algorithm is more obvious and closer to the optimal solution. At the same time, the search speed of the improved ant colony algorithm is also further faster than that of the ant colony algorithm to some extent. For large-scale network, the search speed of the improved ant colony algorithm will not slow down in the later period. In the above five scale attack graphs, the search speed of the improved ant colony algorithm is 8.62% higher than that of the ant colony algorithm on average, and the highest efficiency is three times than that of other methods. Also, it is found that, in the case of many attack paths, the improved ant colony algorithm improves the search speed optimization more obviously and is more suitable for large-scale network.

In this section, the concept of minimum critical attack set (MCPS) is first expounded, and then, it is proved that the solution of MCPS can be equivalent to the solution of NP-complete problem. Ant colony algorithm (ACO) is widely used in solving NP complete problems. However, it is found in the further solution that ACO tends to converge prematurely in the solution process, which often leads to convergence at the local optimal solution and makes the algorithm stagnate instead of getting the global optimal solution. Therefore, this paper proposes an improved ant colony algorithm in the fourth section, which uses the adaptive update of pheromone to optimize the selection of the next node and uses the adaptive genetic algorithm to improve the local search strategy. In the final experimental analysis, the results show that the improved ant colony algorithm has a significant improvement in solving the problem of the minimum critical attack set and in searching speed under different network sizes. Especially when the scale of attack graph increases gradually, the effect of solving accuracy and solving time becomes more obvious, and it is more suitable for large-scale network. Most of the time vulnerabilities and their disclosure are due to poor system management, late patching, weak password policies, inadequate access control mechanisms, and so on. Therefore, the primary reason and purpose of penetration testing should be to identify and correct failures in the system management process that lead to the emergence of system vulnerabilities that are disclosed during penetration testing. The method presented in this paper can effectively avoid such leakage.

Many cities begin to introduce intelligent transportation facilities into the urban transportation construction, which can not only guarantee people's travel more smoothly but also further promote the development and progress of the transportation field. Although intelligent transportation has begun to be effectively applied to cities, as the urban population surges, many rural people go to cities to work, making the development of

FIGURE 11: The minimum critical attack set can be solved for attack graphs of different scales.

intelligent transportation difficult to withstand the ever-expanding traffic pressure in cities. It can be found that the traffic conditions of many cities in our country are very tight, and the traffic pressure problem is increasingly aggravating. In order to make the intelligent transportation system better meet the needs of the city, the transportation system and the Internet of Things should be organically combined, so that the Internet of Things technology can be applied scientifically and the transportation facilities can realize the joint application of the intelligent transportation system and solve the problems faced by the urban transportation.

5. Conclusion

Nowadays, computer technology has entered our daily life, so it is urgent to protect and maintain network security. However, in the face of the diversity and complexity of the attack means of the attackers on the network, our security protection measures have a certain lag. In the final analysis, the problem of network security is due to the existence of vulnerability loopholes in the network system, which gives attackers an opportunity to take advantage of. Therefore, in order to be able to develop better preventive measures in the network security protection system, we should start from the analysis of the vulnerability vulnerabilities in the network system. Therefore, this paper focuses on the network security evaluation and analysis based on the attack graph model. Attack graph technology can analyze the vulnerability of each host in the network, find out the attack path threatening network security, and show it in the way of directed graph. However, the attack graph generated by large-scale network is too complex and poor in readability, which is difficult for security managers to analyze, thus affecting their accurate security judgment and reinforcement of defense measures. Therefore, the main work of this paper is as follows: using MuiVal attack graph building tool to generate a directed

attribute attack graph. The phenomena of various kinds of loops in attribute attack graph are explained in detail, and the general methods of eliminating loops are expounded. An optimization algorithm based on path complexity is implemented for the attack graph after eliminating the loop. The attack graph can be optimized to different degrees by using the formula of attack distance and atomic weight and setting different values. Finally, the effectiveness of the proposed algorithm is verified by an experiment based on a specific network topology. On the basis of simplifying the attack graph, the network environment is strengthened with the minimum cost. Firstly, the concept of minimum critical attack set (MCCS) is expounded, and then, it is proved that solving the MCCS is equivalent to solving the NP problem. According to ant colony algorithm, the problem of early convergence and late search is too slow in solving the minimum critical attack set so that only the local optimal solution can be obtained. Based on ant colony algorithm, this paper proposes to improve ant colony algorithm by using adaptive updating principle of pheromone and local search strategy. Finally, the simulation experiment is used to compare the two algorithms in the approximate solution speed and the number of sets.

Data Availability

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Consent

Informed consent was obtained from all individual participants included in the study references.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

References

- [1] M. H. R. Khoisan, L. Zhenjiang, and M. Pasquale, "Scalable min-max multi-objective cyber-security optimisation over probabilistic attack graphs," *European Journal of Operational Research*, vol. 278, no. 3, pp. 894–903, 2019.
- [2] H. Hu, J. Tan, and J. Liu, "SOCMTD: selecting optimal countermeasure for moving target defense using dynamic game," *KSI Transactions on Internet and Information Systems (TIIS)*, vol. 14, no. 10, pp. 4157–4175, 2020.
- [3] M. Stolpe, "The internet of things," *ACM SIGKDD Explorations Newsletter*, vol. 18, no. 1, pp. 15–34, 2016.
- [4] E. D. Pontiki, "Multi-target cinnamic acids for oxidative stress and inflammation: design, synthesis, biological evaluation and modeling studies," *Molecules*, vol. 24, no. 1, p. 12, 2019.
- [5] A. O. Akmandor, H. Yin, and N. K. Jha, "Smart, secure, yet energy-efficient, Internet-of-Things sensors," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 4, no. 4, pp. 914–930, 2018.
- [6] G. Spanos and L. Angelis, "A multi-target approach to estimate software vulnerability characteristics and severity scores," *Journal of Systems and Software*, vol. 146, no. 7, pp. 152–166, 2018.
- [7] L. Yuqing, "An intelligence-driven security-aware defense mechanism for advanced persistent threats," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 646–661, 2018.
- [8] M. O. Al Kalaa and H. H. Refai, "Monitoring radiated co-existence testing using GMM-based classifier," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10336–10345, 2017.
- [9] S. Thöns, M. G. Stewart, and G. S. Mark, "On decision optimality of terrorism risk mitigation measures for iconic bridges," *Reliability Engineering & System Safety*, vol. 188, no. 13, pp. 574–583, 2019.
- [10] P. Lau, W. Wei, L. Wang, Z. Liu, and C.-W. Ten, "A cybersecurity insurance model for power system reliability considering optimal defense resource allocation," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 4403–4414, 2020.
- [11] A. R. Sourì, "A state-of-the-art survey of malware detection approaches using data mining techniques," *Human-centric Computing and Information Sciences*, vol. 8, no. 1, pp. 1–22, 2018.
- [12] A. R. Kumar and A. Sivagami, "Security aware multipath routing protocol for WMSNs for minimizing effect of compromising attacks," *Journal of Network and Systems Management*, vol. 27, no. 3, pp. 573–599, 2019.
- [13] S. Velliangiri, "A hybrid BGWO with KPCA for intrusion detection," *Journal of Experimental & Theoretical Artificial Intelligence*, vol. 32, no. 1, pp. 165–180, 2020.
- [14] G. Tao and Q. Zhang, "Research on smart grid energy internet of things technology and network security," *IOP Conference Series: Materials Ence and Engineering*, vol. 677, no. 4, pp. 42–117, 2019.
- [15] J. Wang, A. Liu, and T. Yan, "A resource allocation model based on double-sided combinational auctions for transparent computing," *Peer-to-Peer Networking and Applications*, vol. 11, no. 4, pp. 612–633, 2018.
- [16] X. Feng, H. Zhang, and Y. Ding, "A review study on traction energy saving of rail transport," *Discrete Dynamics in Nature and Society*, vol. 2013, no. 1, pp. 1611–1617, 2013.
- [17] V. Miori, D. Russo, and L. Ferrucci, "Supporting active aging through a home automation infrastructure for social internet of things," *Advances in Science, Technology and Engineering Systems Journal*, vol. 3, no. 4, pp. 173–186, 2018.
- [18] A. Aliverti, "Wearable technology: role in respiratory health and disease," *Breathe*, vol. 13, no. 2, pp. e27–e36, 2017.
- [19] A. Manocha, R. Singh, and P. Verma, "An internet of things fog-assisted sleep-deprivation prediction framework for spinal cord injury patients," *Computer*, vol. 53, no. 2, pp. 46–56, 2020.
- [20] M. S. Mahmud, H. Fang, and H. Wang, "An integrated wearable sensor for unobtrusive continuous measurement of autonomic nervous system," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 1104–1113, 2018.