Attack path analysis of power monitoring system based on attack graph

Xiaojian Zhang1*, Qi Wang2, Xiangqun Wang2 and Run Zhang3

1Global Energy Interconnection Research Institute Co .Ltd, Nanjing, Jiangsu,210003, China
2State Grid Key Laboratory of Information & Network Security, Jiangsu, Nanjing 210003, China
3 Beijing University of Posts & Telecommunications, Beijing, 100876, China
*Corresponding author’s e-mail: zhangxiaojian@geiri.sgcc.com.cn

Abstract. Power monitoring system, as the key to ensure the normal operation of power, is facing huge security threats. The existing protection measures for power monitoring systems mostly start from the aspect of early warning, instead of actual penetration testing of the power monitoring system. To solve this problem, a path analysis method of power monitoring system based on attack graph is proposed to simulate the security test of power monitoring system. In the aspect of route selection, this project quantifies the attack benefits and attack costs to obtain the attack efficiency on each path, and then applies the ant colony algorithm with high efficiency to select the attack path.

1. Introduction
In recent years, the target of attackers has gradually shifted from the common computer network to the industrial control network. Power monitoring system is a kind of industrial control system, which is used to monitor and control the power production and supply process. And it faces the severe security situation.

At present, most of the protection for power monitoring system only stays at the monitoring level[1,2,3,4]. There are a few researches on optimizing electric power monitoring system, and the method of optimizing the system only involves using scanning tool to detect the vulnerability, and fix system vulnerabilities[5]. However, this method ignores the correlation between the vulnerability and has a high rate of missing report and false alarm.

To better solve these problems, and to improve the security of power monitoring system, this paper designed an attack path analysis method of power monitoring system based on attack graph. This paper uses attack graph to correlate vulnerable points in the system. Before the path selection, the attack path should be quantified. After that ant colony algorithm is used to select the path with the highest attack efficiency, so as to provide reference for the subsequent security reinforcement work.

2. Related work
Zhang H. et al. [1] analyzed and processed the alarm information in the system, and found the possible attack path by generating the alarm map to carry out more accurate early warning. Chen L. et al. [4] studied the attack efficiency in attacks from communication networks to physical networks, and obtained the best attack path by analyzing the attack cost and attack gain and using Floyd-Warshall algorithm.
However, this kind of research aimed at improving the performance of intrusion detection system can only reduce the rate of missed alarm and false alarm, so as to provide alarm information in a timely manner, without testing and analyzing the security of the system itself, it cannot fundamentally solve the problem.

On the basis of ant colony algorithm, Thomas et al. [6] limited the pheromone change and the upper and lower limits of volatilization, and to a certain extent avoided the problem of easily falling into the local optimal solution. Fonseca et al. [7] proposed a sorting based pheromone updating strategy, which improved the feedback effect of ants and thus improved the convergence speed and quality of ant colony algorithm. Cao et al. [8] attempted to apply ant colony algorithm to robot path planning, and prospected future research hotspots.

3. Attack path analysis model of power monitoring system

Firstly, this paper generates an attack graph based on the vulnerability and communication relationship in the power monitoring system, and then analyzes the cost and value of exploiting the vulnerability in each path, and then estimates the difficulty of jumping between nodes, so as to conduct path quantification. On this basis, ant colony algorithm is used to analyze the attribute attack graph of power monitoring system, and the path with the highest attack efficiency is obtained.

3.1. Attribute attack graph of power monitoring system

In the attack graph, vulnerability number is often used as a node to represent the attack process together with the attack benefit. However, the same vulnerability may correspond to multiple atomic attacks, and the attack cost and attack benefit caused by different atomic attacks are different, which makes it impossible to reflect the invasion situation comprehensively and accurately by using the vulnerability number alone. Therefore, this paper uses regular expressions to extract the key information in the description of vulnerability, gives the corresponding attack pattern of vulnerability and adds it to the attack graph. An example of the attack graph used in this article is shown in Figure 1.

![Figure 1. attack chain of a single node](image)

3.2. Path quantization of power monitoring system

The Common vulnerability Scoring system (CVSS) is a common reference for researchers to evaluate the vulnerability and attack benefit, but the attack effect of industrial controlled network is not the same as that of normal computer network. Therefore, the original CVSS scoring equation is not applicable to this kind of network, and may even seriously mislead the security operation and maintenance work. To solve this problem, this paper proposes a cost and benefit quantization method based on vulnerability chain, and finally gives the path quantization score.

As shown in Figure 1, CVE-2017-8463 vulnerability is first utilized in the penetration process to enable the attacker to execute malicious code remotely. Then, the permission can be enhanced through CVE-2016-5195, or sensitive information can be obtained through CVE-2017-1131.

The cost quantization value of a node is determined by the cost of multiple atomic attacks used at the time of the invasion, and the cost of each atomic attack can be inferred from the dimensions of attack complexity, code utilization maturity, and so on.

In this paper, the atomic attack cost calculation equation is presented as follows:
Cost_{attack}=(AC*AV*PR)^{CM} \hspace{1cm} (1)

The calculation equation of attack cost is as follows:

Cost_{node} = \sum_{i=0}^{k} Cost_{ai} \hspace{1cm} (2)

In the equation, AC is vulnerability complexity, AV is attack vector, PR is permission requirement, CM is code utilization maturity.

This paper also deduces the benefits of atomic attacks, in which the measurement criteria of the benefits of attacks are evaluated according to the impact of attacks on the confidentiality, integrity and availability of information systems as well as the permissions obtained, respectively using \( C \cdot I \cdot A \) and \( PO \), as shown in equation (3):

\[
\text{Influence} = (\text{Inf}_C, \text{Inf}_I, \text{Inf}_A, \text{Inf}_PO)
\]

As different industrial control networks have different security requirements for each item, the following weight coefficient vectors are defined in equation (4) according to the security focus of the power monitoring system.

\[
\omega = (w_C, w_I, w_A, w_PO)
\]

This paper uses the weight coefficient vector to calculate atomic attack benefits BF shown in equation (5):

\[
BF = w_C \cdot \text{Inf}_C + w_I \cdot \text{Inf}_I + w_A \cdot \text{Inf}_A + w_PO \cdot \text{Inf}_PO
\]

The generated attack graph covers as much vulnerability information as possible, so unnecessary atomic attacks may occur during the intrusion of a single node. For example, the sensitive information disclosure vulnerability in Figure 1. Therefore, this paper proposes the concepts of a minimum set of vulnerabilities and a maximum set of vulnerabilities, and applies them to the quantization process of nodes. The minimum set of vulnerabilities is the set of vulnerabilities necessary to control the target. The maximum set of vulnerabilities is the set of vulnerabilities required to obtain the maximum operating space. The maximum vulnerability set is the vulnerability set that can obtain the maximum resources and permissions. In Figure 1, the minimum set is shown in (6) and maximum set of vulnerability is shown in (7)

\[
V_{min} = \{\text{CVE-2017-8464}, \text{CVE-2016-5195}\} \hspace{1cm} (6)
\]

\[
V_{max} = \{\text{CVE-2017-8464}, \text{CVE-2016-5195}, \text{CVE-2017-1131}\} \hspace{1cm} (7)
\]

The quantization equation of the attack path is shown in equation (11)

\[
\text{score}_{node} = \max \left\{ \frac{BF_{max}}{Cost_{max}}, \frac{BF_{min}}{Cost_{min}} \right\} \hspace{1cm} (8)
\]

3.3. Attack path selection algorithm

As for path selection algorithm, this paper chooses ant colony algorithm which can perform positive feedback and heuristic search to select the optimal path.

Different from the common ant colony algorithm, the ant colony algorithm used in this paper only has one starting point, that is, the attack starting point of the attacker, the ant trajectory does not constitute a loop, it does not require each ant to traverse all vertices, and it solves the longest path problem. In the algorithm used in this paper, the host is regarded as the city, using \( \tau_{ij}(t) \) to represent the pheromone concentration on the route \( ij \) at time \( t \). During ant movement, pheromone will gradually increase on each attack path. In the attack of power monitoring system, the attacker usually takes the control permission of the monitoring terminal as the ultimate goal. Therefore, this paper takes the control terminal node as the nest. In addition to pheromone concentration, the choice of ant homing path is also affected by heuristic function. In this paper, the value of the heuristic function is the quantized value of
the node, namely the ratio of attack cost to attack benefit. Equation (9) indicates the probability of node
$j$ being selected by ant $k$. It should be noted that in this paper, $J_k(i)$ is the set of nodes that can be reached
from Node $I$, which is generated according to the node connectivity matrix $A_I$, with element 1 representing reachable and element 0 representing unreachable. After a round of ant crawling, the
maximum and minimum ant colony algorithm (MMAS) was used to update the pheromone concentration, that is, only the pheromone concentration on the optimal path was increased, while the pheromone concentration on other paths was reduced according to the parameters. Equations 11 and 12
give the updating equations of pheromones on the optimal path, while equation 10 gives the updating
equations of pheromones on other paths.

$$P_{ij}^k(t) = \frac{[\tau_{ij}(t)]^\alpha [\eta_{ij}]^\beta}{\sum_{s \in J_k(i)} [\tau_{is}(t)]^\alpha [\eta_{is}]^\beta}$$ (9)

$$\tau_{ij}(t+1) = \tau_{ij}(t)(1-\rho)$$ (10)

$$\tau_{ij}(t+1) = \tau_{ij}(t)(1-\rho) + \sum_{k=1}^{m} \Delta \tau_{ij}^k$$ (11)

$$\Delta \tau_{ij}^k = \begin{cases} Q \text{ ant } k \text{ went through path } ij \\ 0 \end{cases}$$ (12)

At this point, we successfully integrate ant colony algorithm and attack path selection algorithm.

4. Experiment

In this paper, combined with the characteristics of power monitoring system, the following experiments
are designed to verify the advantages of this method.

The network topology shown in Figure 2 is a simple power monitoring system model, and the
information of terminals and vulnerabilities in each region is shown in Table 1.
Table 1. Equipment and vulnerabilities in power monitoring system

| Zone                  | Terminal Name | IP Address     | Vulnerabilities                                      |
|-----------------------|---------------|----------------|-----------------------------------------------------|
| Office Zone           | Host 1        | 192.168.55.1   | CVE-2018-0741, CVE-2018-0758, CVE-2018-0742       |
|                       | Host 2        | 192.168.55.120 | CVE-2016-1985, CVE-2018-0744, CVE-2016-1505       |
| Demilitarized Zone    | FTP Server    | 192.168.10.1   | CVE-2016-10102, CVE-2016-1440                       |
|                       | Web Server    | 192.168.10.2   | CVE-2018-1000024, CVE-2016-1002, CVE-2017-1087    |
| Data Center           | Data Server   | 10.20.7.1      | CVE-2015-0016, CVE-2017-14089                       |
| Monitoring Zone       | Monitoring    | 10.20.1.1      | CVE-2016-0010, CVE-2016-7257, CVE-2017-2789, CVE-2018-0743 |
|                       | Printer       | 10.20.6.1      | CVE-2017-2750, CVE-2016-7257, CVE-2017-2789, CVE-2018-0743 |

Network communication with the master station layer were isolated from the firewall, traffic from the network communication layer can reach the web server and DMZ host 1 in the office zone, Host 1 can access host 2, the Web server in DMZ zone and FTP server are in the same subnet, the host in the office zone can access the FTP server, host 2 can access the data server in the data center, the printer and monitoring terminal in the monitoring zone can access the data server, and the monitoring terminal can access the printer.

The attack graph generated by the algorithm in this paper is shown in Figure 4.

![Figure 4. Power monitoring system attack graph](image)

The path quantization values calculated according to the equation in Section 3.2 are shown in Table 2.
Table 2. Path quantization value

| Source       | Destination | Maximum set quantization value | Minimum set quantized value | Final quantized value |
|--------------|-------------|-------------------------------|-----------------------------|-----------------------|
| Internet     | 192.168.10.2| 5.09                          | 4.90                        | 5.09                  |
| 192.168.10.2 | 192.168.10.1| 6.82                          | 9.19                        | 9.19                  |
| Internet     | 192.168.10.1| 5.58                          | 5.96                        | 5.96                  |
| 192.168.10.1 | 192.168.10.1| 4.04                          | 4.04                        | 4.04                  |
| 192.168.55.1 | 192.168.55.1| 3.38                          | 2.68                        | 3.38                  |
| 192.168.55.1 | 192.168.55.120| 4.04                       | 24.10                       | 24.10                 |
| 10.20.7.1    | 10.20.6.1   | 24.10                         | 24.10                       | 24.10                 |
| 10.20.6.1    | 10.20.1.1   | 4.09                          | 3.92                        | 4.09                  |
| 10.20.7.1    | 10.20.1.1   | 3.40                          | 3.40                        | 3.40                  |

In this experiment, the maximum iteration number is 3, the pheromone volatility coefficient is 0.9, the ant colony number is 30, the pheromone bias degree is 1, and the importance degree of the heuristic factor is 3, namely

\[ \text{Iternum} = 3, \ \rho = 0.9, \ m = 30, \ \alpha = 1, \ \beta = 3 \]

The results of algorithm operation in this paper are shown in Figure 6, and the longest path length is 78.64. The results show that the attackers have the highest attack efficiency along the attack sequence of Web server → FTP server → host 1 → host 2 → Data server → transaction printer → monitoring terminal. The administrator should reinforce the device on this path, and at the same time, the corresponding attack mode and vulnerability in the attack diagram can be referred to for hardware upgrade or download the repair program.

5. Conclusion

In this paper, a vulnerability analysis method for power monitoring system is designed. Firstly, the attack patterns corresponding to each vulnerability are analyzed through the possible vulnerabilities on the equipment, and the attack benefits of each vulnerability are deduced by using the attack patterns, and then the attribute attack graph is formed according to the vulnerability utilization conditions and attack benefits. Then the utilization cost is obtained by analyzing the vulnerability utilization degree. Then, by analyzing the possible consequences and harms caused by atomic attacks, the quantized attack benefits can be obtained, and the final path quantization value can be obtained by analyzing the minimum set and the maximum set. Finally, the idea of ant colony algorithm is used, and combined with the feature of attribute attack graph with single starting point and multiple targets, the path with the most possibility of being exploited by the attacked in the attack graph is obtained.

The next step is to further improve the attack graph generation method and ant colony algorithm. The introduction of richer vulnerability information into the attack diagram, such as the protocol vulnerability information unique to the power monitoring system, can improve the accuracy of attack path prediction and provide better Suggestions for subsequent security improvement. In addition, the analysis method designed in this paper is mainly used for power monitoring system, industrial control system, isolated internal network and other scenarios. In the future, different quantitative standards will be equated and according to the characteristics of each system scenario, so as to improve the pertinence of special networks.

Acknowledgments

This work was supported by the science and technology project of State Grid Corporation of China "Development of special cyber security toolbox for electric power supervisory and control system" (Grand No. 525500190016).

References

[1] Zhang, H., Jin, X.Q., Li, Y., Jiang, Z.W., Liang, Y., Jin, Z.P., Wen, Q.Y. (2020) A Multi-Step Attack Detection Model Based on Alerts of Smart Grid Monitoring System. IEEE Access, 8: 1031-1047.

[2] Wang, J., Zhong, Z.M., Lu, C.B. (2020) Research on advanced Persistent Threat Perception of
[3] Li, Z.K., Chen, Z.W., Wang, C.Y., Xu, Z.G., Liang, Y. (2020) Research on network Security Threat Traceability technology of power Monitoring System. Power engineering Technology. 39:166-172.

[4] Chen, L., Yue, D., Dou, C., Chen, J., Cheng, Z. (2020) Study on attack paths of cyber attack in cyber-physical power systems. IET Gener. Transm. Distrib., 14:2352-2360.

[5] Wei M.X. (2017) Research on the construction of network security attack and defense range system in power monitoring system. Front. Artif. Intell. Appl. 296:82-90.

[6] Stützle, T., Hoos, H. H. (2000) MAX–MIN ant system. Future generation computer systems, 16:889-914.

[7] Fonseca, L. G., Capriles, P. V., Barbosa, H. J., Lemonge, A.C. (2007). A stochastic rank-based ant system for discrete structural optimization. In: 2007 IEEE Swarm Intelligence Symposium. Honolulu. pp. 68-75.

[8] Cao, M., Yang, Y., Wang, L. (2019). Application of Improved Ant Colony Algorithm in the Path Planning Problem of Mobile Robot. In: 2019 3rd High Performance Computing and Cluster Technologies Conference. Xi'an. pp. 11-15.