Journal of System Simulation

Volume 29 | Issue 10 Article 35

6-4-2020

Brief Technical Analysis of Malicious Cyber Attacks in Power System

Yan Ru
Shanghai University, School of Mechatronic Engineering and Automation, Shanghai Key Laboratory of Power Station Automation Technology, Shanghai 200072, China;

Minrui Fei
Shanghai University, School of Mechatronic Engineering and Automation, Shanghai Key Laboratory of Power Station Automation Technology, Shanghai 200072, China;

Dajun Du
Shanghai University, School of Mechatronic Engineering and Automation, Shanghai Key Laboratory of Power Station Automation Technology, Shanghai 200072, China;

Brief Technical Analysis of Malicious Cyber Attacks in Power System

Abstract

Abstract: The power system is responsible for providing electric power to the society. Whether its operation is safe and reliable or not is directly related to the economic livelihood and national security. *The malicious cyber-attacks happening on power systems in recent years were summarized, the attack methods used in malicious attack were enumerated, and the complexity and diversity of attack methods were analyzed.* The vulnerability of the power system at present was pointed putting forward the corresponding measures to ensure the safe and stable operation of power system. Experimental simulation is designed to analyze the attack methods. The future research directions were briefly introduced.

Keywords

power system, cyber attack, security vulnerability, malicious cyber attacks, defense

Recommended Citation

Yan Ru, Fei Minrui, Du Dajun. Brief Technical Analysis of Malicious Cyber Attacks in Power System[J]. Journal of System Simulation, 2017, 29(10): 2507-2517.

第 29 卷第 10 期 系统仿真学报© Vol. 29 No. 10
2017 年 10 月 Journal of System Simulation Oct., 2017

Brief Technical Analysis of Malicious Cyber Attacks in Power System

Yan Ru, Fei Minrui, Du Dajun
(Shanghai University, School of Mechatronic Engineering and Automation,
Shanghai Key Laboratory of Power Station Automation Technology, Shanghai 200072, China)

Abstract: The power system is responsible for providing electric power to the society. Whether its operation is safe and reliable or not is directly related to the economic livelihood and national security. *The malicious cyber-attacks happening on power systems in recent years were summarized, the attack methods used in malicious attack were enumerated, and the complexity and diversity of attack methods were analyzed.* The vulnerability of the power system at present was pointed putting forward the corresponding measures to ensure the safe and stable operation of power system. Experimental simulation is designed to analyze the attack methods. The future research directions were briefly introduced.

Keywords: power system; cyber attack; security vulnerability; malicious cyber attacks; defense

针对电力系统蓄意攻击的简要技术分析

闫茹，费敏锐，杜大军

（上海大学机电工程与自动化学院，上海市电站自动化技术重点实验室，上海 200072）

摘要：电力系统担负着为社会各行各业提供电能的重要责任，它能否安全可靠地运行直接关系到经济民生和国家安全。*总结了近年来世界各地针对电力系统的蓄意网络攻击事件，对攻击事件的攻击流程和结果进行了简要分析，对各个攻击事件的特点进行了对比研究，分析了针对电力系统的蓄意攻击所采用的攻击手段的复杂性和多样性。*分别阐述了目前电力系统的安全漏洞并提出了相应的防御措施来保证电力系统安全稳定的运行，设计实验仿真来分析研究攻击的方法并对未来的研究方向进行了展望。

关键词：电力系统；网络攻击；安全漏洞；蓄意攻击；防御
中图分类号：TP393.08 文献标识码：A 文章编号：1004-731X (2017) 10-2507-11
DOI: 10.16182/j.issn1004731x.joss.201710035

Introduction

The power system is responsible for providing electricity to all the society, whether it can operate safely and reliably which is directly related to economic people's livelihood and national security. Power systems often suffered from malicious attacks, so that the study about the vulnerability of cyber attacks on power system will become more important, at the same time, we also need to find out what kind of defenses should be used to ensure the safety and reliability of the power system. Therefore, it is of great theoretical and practical significance to analyze the security of power system under the threat of cyber attack.

Received: 2017-05-20 Revised: 2017-07-19;
Foundation item: National Natural Science Foundation 61633016), Shanghai Science and Technology Commission International Science and Technology Cooperation Project (15220710400);
Biography: Yan Ru (1991-), Shanghai, China, Graduate student, Research direction for the smart grid network security.

Network control system, compared with the traditional control system, it has larger scale, and its structure is more complex, when a failure occurs, the loss will be difficult to estimate for it has a lot of uncertain factors, so the power system requires higher security performance. Now the internet is more open, not only the traditional network virus can use the internet to speed up its spread and expand the scope of its spread, and a variety of new approaches to network protocols and application vulnerabilities are emerging.

The smart grid technology is being built on the basis of traditional physical power network at present. It integrates advanced information technology, measurement technology and control technology to ensure the accuracy, reliability, safety, economy and efficiency of the operation. Compared with the existing power grid, smart grid achieved to combine the advanced information technology and traditional power technology together, which pointed out the development direction of power system.

The electric power industry is very important for its safe and reliable operation. In recent years, with the development of smart grid technology, information technology and military technology, the power system is more and more likely to be attacked by the hackers. Compared with the random cyber attacks, malicious cyber attacks cause a greater threat to the power system. Therefore, it is an important problem to study the data security vulnerabilities and formulate corresponding defensive measures in the actual power system [1- 4].

1 Analysis of Cyber Attack Events

The cyber attack get into the power monitoring system, power communications and data networks through the connection between the networks. Attackers focus on destroying or reducing the function of the power system. They attack the power systems and resources by attacking and disturbing the digital relay protection devices, fault recorder, automatic devices, station control layer computer, programmable logic controller and other electronic devices and communication interfaces. The complexity of the cyber attack mechanism, the performance of different sources of attackers and the complexity of the attack methods make it difficult to predict the attack results [5-10].

By summarizing the cyber attacks happened in the power system in recent years, we can analyze the characteristics and means of malicious attacks, and deepen the understanding of malicious attacks and facilitate the follow-up research[11-12].

1.1 Summary analysis of the large-scale power system cyber attack in recent years

The large-scale power outage caused by cyber attacks in recent years was listed, a brief explanation was made of attack techniques and attack process. And Tab.1 shows the details of all the events.

1.1.1 Ohio nuclear power station suffered worm invasion in 2003

In January 2003, the Davis-Besse nuclear power plant and other electrical equipment in Ohio were attacked by the SQL Slammer worm, which exploited the buffer overflow vulnerability of 1434 ports in SQL Server 2000, causing the network to be congested and some of the units were out of service. This cyber attack event causes other line load and the total power supply continues to reduce which triggered a series of accidental chain reaction, eventually lead the system to the final collapse.

The investigation found that the application software which the supplier provides to the server built an unprotected T1 link at the back end of the network firewall in the plant, where the virus entered the nuclear power station network through this link.

DOI: 10.16182/j.issn1004731x.joss.201710035

Tab. 1 Malicious cyber attacks of power systems around the world in recent years

Year	Country	Virus	Attack Method	Influence
2003	United States	Slammer virus	Firewall vulnerability, 1434 port buffer overflow vulnerability in SQL Server 2000	The computer processing speed is slow and the display system does not work for hours. 61800MW load loss, 50 million people suffered power outage, resulting in economic losses of 30 billion US dollars
2006	United States	Information flood attack	Frequency converter (VDF) for adjusting the speed of the circulating pump motor and the programmable logic controller (PLC) for condensing and removing the mine can not be processed in time	Browns Ferry nuclear power plant unit 3 was attacked, causing the reactor to recirculate the pump and the condensate de-mining controller failed to work, and the nuclear reaction equipment was paralyzed
2010	Iranian	Earthquake virus	4 vulnerabilities in Microsoft system, three of them are 0day vulnerabilities	Causing the system to paralyze the network, the Iranian centrifuge run out of control, and cover up the failure of the situation to "normal operation" and make up records to send back to the management department, resulting in misjudgment of decision-making
2011		Duqu virus	lurk to collect a variety of information about the targets for future attacks	
2015	Ukraine	Black Energy	Deleting data from the computer's disk drive and lead to restart failure of the system	Resulting in about 1.4 million people out of power for 3~6 hours, hit the SCADA system and a large number of stored data is cleared
2016	Israeli		Aim at the infrastructure, and affect its normal operation	Part of the power network is off, part of the computer shut down for two days and cannot operate

1.1.2 Alabama's Browns Ferry Nuclear Power Plant was attacked in 2006

In August 2006, the Browns Ferry Nuclear Power Plant unit in Alabama, USA, was attacked by the hackers, and the reactor recirculation pump and condensing and dewatering controller failed to work, causing the Unit 3 shut down.

This unit has two microprocessors embedded in the frequency converter (VFD) that regulates the speed of the recirculating pump motor and in the programmable logic controller (PLC) for condensing and deinking. By using the microprocessor, the VFD and PLC can accept broadcast data communication in an Ethernet LAN. However, due to the emergence of the information flood that day the nuclear power plant LAN, VFD and PLC cannot progress the data, resulting in paralysis of all the devices[13].

1.1.3 Earthquake virus in 2010 caused Iranian nuclear facilities to fail

Earthquake virus appeared in 2010 shocked the world, it infected more than 45,000 networks through worldwide. The virus takes the use of at least four loopholes in the Microsoft operating system, including three new zero-day loopholes. Earthquake virus has a complete invasion and propagation process, it breaks the industrial dedicated LAN physical constraints and takes the use of two loopholes of Windows system to carry out its destructive attacks. It is the first malicious code that directly destroys the industrial infrastructure in the real world. Earthquake virus can establish a botnet in which the infected computers will continue to send the virus to other uninfected computers, and it can use the infected computers to decipher uninfected computer's network port.

1.1.4 Duqu virus was found in 2011

In 2011, some security expert detected a new variant of the Stuxnet virus, called Duqu virus, which is smarter and more powerful than the Stuxnet virus. Unlike the Stuxnet virus, the Duqu Trojan virus is not intended to break the industrial control system, but to lurk and collect information about the target and prepared for the future cyber attacks. Not long ago, some enterprises declared that they have found Duqu code in their facilities too, which means some attack events may occur some day in the future[14].

1.1.5 Ukraine grid was attacked in 2015

December 23, 2015, the Ukrainian National Grid was attacked by a malicious software called "BlackEnergy". This attack caused nearly half of the households in Ivano-Frankovsk (about 140 million people) lost power for 3~6 hours. In this attack, the software adds a cleanup component called KillDisk to remove data from the computer's disk drive which causes the system fail to restart, and the attacker uses the Dos attack to limit the user's data reporting. This attack indicates that the hackers are well-prepared and they have aimed at the Ukraine national grid for a long time[15].

In this incident, the Supervisory Control and Data Acquisition (SCADA) system was attacked, a large number of stored data were cleared from it, which seriously affected the later recovery. On December 23, the Ukrainian power grid's power outage was seen as the first occurrence of the malicious cyber attack against the power supply system, which caused thousands of Ukrainian people into a powerless dilemma[16-17].

After this, the malicious software takes the place of virus and becomes the major attack techniques, which is more complex. The appearance of the malicious software put the security of power systems in an essential position.

1.1.6 Israeli power grid was attacked in 2016

The large-scale cyber attacks happened on the Israeli national grid have caused the country's electricity supply system to be hit seriously, and several reports have shown that extortion software is the direct cause of the accident.

As can be seen from Table 1, the cyber attacks in these years show that network viruses and malware are continually improving for better attacking effect of power systems. The purpose of the cyber attack against the power system is more and more obvious, the attack technique is more and more accurate, the consequences of it are more terrible, and more and more networks are affected.

1.2 Characteristics of cyber attack for power system

The power system malicious cyber attacks can destroy and change the hardware, system software and data of the power system, so that system cannot maintain normal and reliable operation, resulting in the interrupt of the internal network service system, and causing widespread power outages. At present, the cyber attacks for power systems have the characteristics of clearer targets, more attacks techniques and wider range of influence.

1.2.1 A malicious attack with a clear target

According to the analysis of the existing situation, we can see that the hackers destroy the power system for a purpose. Which can be seen through the analysis of the previous cases is that most attackers have a very well understanding of the composition and structure of the target system. In order to maximize the effect of attack, before the attack, the hackers will take some time to collect the information about the target, which means they may have a certain understanding of the infrastructure of

DOI: 10.16182/j.issn1004731x.joss.201710035

the power system. The better understanding and analysis of the power system structure and a well-made attack plan designed step by step, make the attack process quite careful and a better attack effect. Every step of the attack has a clear intention and technology background, the previous step of the attack protects and at the same time paves the way for the next step, thus resulting in the whole power system failure.

1.2.2 The scope of the attack were more extensive

The target of cyber attack of the power system is the secondary part of power system and acts on the primary power infrastructure, the technique of attack is with low cost and easy to hide and put into effect. A wide power outage will cause great economic loss and the latter recovery is also relatively difficult. For the power system, a malfunction may lead to a very bad result, so if criminals sabotage the stability of power system, they will produce more serious consequences for the development of the normal and stable operation of the country.

The malicious attacks occurred in Iran power system in 2010 caused a lot of concern over the world. The discovery of the earthquake virus also causes extensive discussion and has bad influence with a wide range of industries, which shows that a new attack technique will not only affect the power system itself, but also will put a threat to all of the network control system[18-19].

1.2.3 Attack methods and means are more complex

With the improvement of complexity of the network control system and the network architecture, the network attack methods are becoming more complex. Most of the current network attacks are coordinated attack, which is a well planned and executed attack behavior, it integrates multiple attacks in the attack process to maximize the effect.

The hackers' attack of Ukrainian power grid is one of the representatives of coordinated attacks. Hackers first sent an e-mail carried a malicious link from which it could load malicious software on the controller's computer, thus affecting the availability of substation monitoring system, making the dispatcher could not remotely monitor the status of substations. And then they got the access to the substation monitoring server operating authority, carried out a malicious switch operation and cut off the load carried by the substation. Hackers also used the denial of service attacks (Dos) on the power company's Web site and customer service system to prevent the user's accident report, and extend the power outage time. Finally, they used the malicious software to rewrite and erase the parameters in the substation monitoring system server and workstation system, not only to hide the important traces of the attack, but also make the monitoring system cannot resume normal operation for a long time.

1.3 Advanced attack methods and techniques used at present

By summarizing cyber attacks of the power system in the recent years, we can see that the methods that the current hacker use to attack the power system can be divided into four kinds, the first one is the usage of the computer vulnerabilities, such as the earthquake virus which uses the 0 day vulnerabilities to get into the computer. The second one is the attack with the communication protocols of the computer system, such as flood attacks, which called denial of services (DoS) often. The third one is to install malicious software on the controller's computer, such as BlackEnergy. The fourth one is to tamper with the control system command, this attack method is more advanced, and hackers need to have a good knowledge background, such as FDIA attack.

1.3.1 Computer vulnerability attack

Computer vulnerability is a flaw in the hardware, software, protocol implementation, or system security policy that allow an attacker to access or destroy the system without authorization. This vulnerability is a missing question of programming in computers, it was not found during debugging and testing, and then the software or hardware was put into use. Hackers used the vulnerabilities of power system applications or other software in the monitor computers to enter the power system, resulting in the damage or downtime of the power equipment.

The problem of newly released software being cracked in a short time is called 0day vulnerability. The existent of a 0 day vulnerability caused the Iran's nuclear power plant failure event mentioned above, resulting in some more serious virus software to get into the control center computers which cause further deterioration.

In theory, loopholes always exist, but have not been found yet, and the compensation measures are always lagging behind. So the operation and maintenance of electrical equipment are quiet essential.

1.3.2 Denial of service attack

Denial of Service (DoS) attack takes the use of the loopholes during the system design or implementation and the attack aims at the system crash or resource exhaustion in order to let the system cannot provide service. Target resources for attack consumption include CPU, memory, hard disk, network bandwidth, and so on. The use of network protocols / software defects or sends a large number of useless requests to exhaust the resources of the attack object (such as network bandwidth) causing the server or communication network cannot provide services.

Distributed Denial of service (DDoS) attacks, as shown in Fig.1, is one of the commonly used resource depletion attacks[20]. The attacker uses his own computer as the proxy host (Host) to send instructions. The host controls the puppet machine (proxy attack) to attack, its distribution is wider, and can attack a larger range with simple techniques. When the power system server is attacked by DoS attack, it will overflow and stop offering services for users[20].

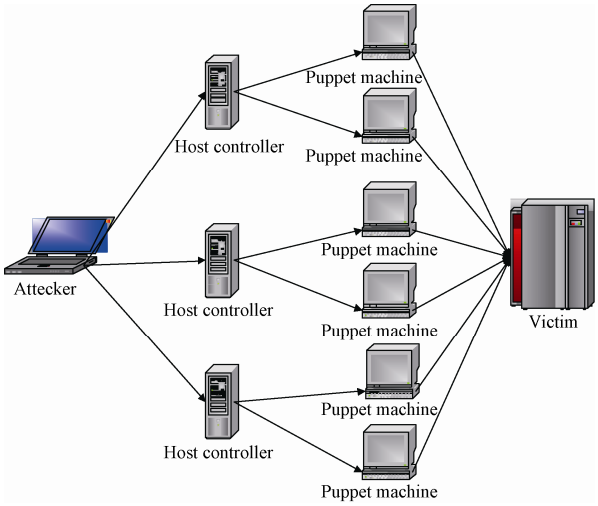

Fig. 1 DDos attack schematic

1.3.3 FDIA

Power system state estimation with false data injection attack (FDIA) can effectively avoid the traditional bad-data detection and identification, which puts the power system safe and reliable operation into a huge threat. The attacker obtains the power system network parameters and topology, and have in-depth study of the relevant state estimation method and vector construction knowledge, so that they can maliciously construct fraudulent data to avoid traditional bad data detection and identification algorithms, and thus deliberately manipulate the results of state estimation, affecting the safe and reliable operation of power systems.

In terms of power system operation control, the

https://dc-china-simulation.researchcommons.org/journal/vol29/iss10/35
DOI: 10.16182/j.issn1004731x.joss.201710035

most direct consequence of implementing FDIA is to influence the on-line state estimation parameters, which affects the identification of bad data and causes the operator to carry out the wrong economic load scheduling and distribution.

Set state estimation model as:

$$z = Hx + v \tag{1}$$

where z is the measured value, H is the corresponding Jacobian matrix, x is the state value to be estimated, v is the measurement error, where the residual of the measured value and the state value is:

$$r = z - \hat{z} = z - H\hat{x} \tag{2}$$

The objective function is:

$$J(x) = [z - Hx]^T [z - Hx] \tag{3}$$

The minimum value of the objective function is solved by the weighted least squares method.

$$\hat{x} = (H^T H)^{-1} H^T z \tag{4}$$

Set the judgment threshold τ, the data is detected, so that:

$$\|r\| = \|z - H\hat{x}\| < \tau \tag{5}$$

FDIA uses the principle above to add a false data vector a, which causes the input data of the state estimate to become:

$$z_a = z + a \tag{6}$$

The resulting state quantity will be biased:

$$\hat{x}_{bad} = \hat{x} + c \tag{7}$$

Where c is the deviation of the state variables after the false data is injected, and the residual after the attack is:

$$\|r_a\| = \|z_a - H\hat{x}_{bad}\| = \|z + a - H(\hat{x} + c)\| = \|z - H\hat{x} + a - Hc\| \tag{8}$$

If the injected malicious data can be met:

$$a = Hc \tag{9}$$

Which can make:

$$J(\hat{x}_{bad}) = J(\hat{x}) \tag{10}$$

The wrong data cause SCADA making the wrong judgments and processing, thus affecting the normal operation of the power system[21].

1.3.4 Malicious software and viruses

Malicious viruses and software get into the control host through network vulnerabilities and improper operations of the operator. The principle of virus attack is to use the link or vulnerability in the computer background to download malicious programs on the operator's computer, it can generate a background client which can infects other computers, and it can connect to an external server, according to the instructions of the external server, the software may take malicious operations, and then by communicate along the network facilities it can infected other host computers.

The cyber attack now is not just using only one kind of attack, as can be seen in the Ukraine power grid attack event, a deliberate cyber attack of the power system is often the result combined of multiple attacks. The existing Advanced Persistent Threat (APT) is a kind of long-term sustainability of cyber attacks against specific targets of attacks using advanced forms of attack, Fig. 2 is a brief picture of APT attack. APT needs to accurately collect the information of the target system before launching the attack. In the process of this collection, this attack will actively pursue the vulnerability of the attack object in its trusted systems and applications, and the APT attack can use these vulnerabilities to set up the required network, and launch the attack. The whole attack technique is quite complex, while the pertinence is strong, the attack is effective, and it is difficult for the system to make a quick and effective response[22].

2 Analysis of Power System Security

With the increasing number of malicious cyber attacks on the power system, the impact of the attack is getting more seriously, and the analysis of the power system security problem is even more

important. It's essential to find out the weak points in power systems and develop strategies to defense.

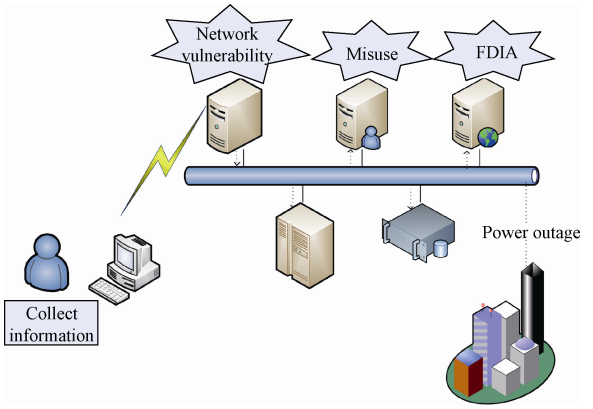

Fig. 2 Malicious network attack graphs

2.1 Causes of Safety Vulnerability in Power Control System

The cyber attacks of power systems show that there are still many shortcomings in the power system at present. There are three main reasons: the protection measures of the power control system are imperfect, the safety awareness of the managers is not strong enough, and the existing network system supervision and management system is not strong[22].

2.1.1 Imperfect protection of power control system

With the combination of information network and physical network in the power systems, problems will be increased in its construction. Because the power physics network is complex and difficult to be managed, the construction of corresponding information network will inevitably encounter problems.

The current information network for the construction of software and communication lines is not perfect. Power system monitoring software and monitoring system cannot accurately control and protect all the physical equipment, and also lack analyzing and processing and making reports of abnormal behaviors. The security of the communication network is insufficient. Unauthorized command and control data can be transmitted on the communication network without authentication which hackers can easily monitored and utilized the current communication network.

2.1.2 Safety awareness of managers is not strong enough

The inappropriate operation of the operator of the power system is also one of the reasons for the potential for security problems in the power system. The installation of inappropriate programs on the host computer, the using of non-dedicated information channel to transmit control commands and signals, the behavior of clicking on the page or link do not confirm their safety with the working computer and so on, these acts will all offer the opportunity for hackers.

Operators of the security with weak awareness may also lead to problems. As can be seen from a number of network information disclosure for the case, some companies and institutions do not have their own user information encrypted, which may cause the hackers stepped into the system and steal the information of the users, and some companies even do not know that they were hacked. Not only that, hackers can even use the leaked information to hide their identity, so it's even more difficult to track them.

2.1.3 Imperfect control systems and supervision system

Power and physical information system is still of development and construction. The construction of smart grid offers a higher request on the existing power system. Now the power system network structure has no corresponding functional safety standards and no establishment of a unified regulatory, and there are no corresponding regulatory

https://dc-china-simulation.researchcommons.org/journal/vol29/iss10/35
DOI: 10.16182/j.issn1004731x.joss.201710035

agencies. In addition, the flexibility of the network also caused more cyber attacks, the supervision and management of hackers are poor, some hackers can easily sell and download the virus software on the Internet, which have a huge security risk.

2.2 Defensive measures against malicious attacks

The number of nodes which is composed of hardware and software in the power network system is large, the structure of the communication network is complex, the interaction process between the systems is also complicated, so it is necessary to put a lot of energy to do the repair work after the attack. With the development of the network defense methods, the attack techniques of the hackers are also constantly improving, a certain means of defense now cannot protect the power system security well. The main goal of power system security defense is to prevent a variety of catastrophic accidents that lead to large-scale power outages[23].

To effectively protect the secondary power system equipment, we must first establish an effective defense mechanism and take preventive measures. Set up a firewall in the power system control system, install the appropriate protection software, analyze and filter the information in the communication line, set up alarm module and security module in the central management unit, analyze and store the real-time information storage, these are all the protection we can do for the power system[24].

An article published in 2000 presented the concept of a Strategic Power Infrastructure Defense system (SPID) [25]. This is a wide-area, intelligent, adaptive protection and control system that allows future power systems to communicate and disseminate information in real time and quickly make judgments and actions for emergencies. In order to prevent the possible occurrence of a variety of malicious cyber attacks, we not only need to enhance the power system's own defense capabilities, but also need to put out rapid and effective solutions when the attack occurred. This is the direction for future research about the malicious cyber attack.

3 Simulation of malicious cyber attack

3.1 Construction of experiment

In order to verify the harmfulness of the above attacks, a simulation attack experiment is designed based on the attack aiming at the control center of the power system. In this paper, we use three softwares to build a DOS attack experiment environment and use two hosts as attackers and victims to complete the simulation.

The attacker set up an attack against the victim under the hacker’s orders. The operator can be considered as a hacker who can launch UDP data attacks. The attacked host is considered as the control center of power system, we can observe the network environment of the host to monitor the attack.

We first use the IP address detection device to locate the IP address of the target. The attack host is then used to attack the target with UDP Flood attack. The data capture tool on the target host used in the simulation can detect the input data and verify the attack.

3.2 Long distance experiments across space

The power network is integrated with the communication network. According to the theory of Dos attack mentioned above, the experiment launched a resource encroachment attack on the control center of network communication, and the

attacks can affect the electrical equipment operations, which will cause the control system fail to issue control command signals and influence the normal operation of power primary equipment.

3.3 Simulation experiment analysis

The IP searcher is used to find the IP address of the target, as can be seen in Fig. 3, assume that the IP address of the controller of a power system is known in a given region, and the other IP addresses can be searched in the neighborhood range based on this IP address, so we can query the network card address of the controller in the same LAN.

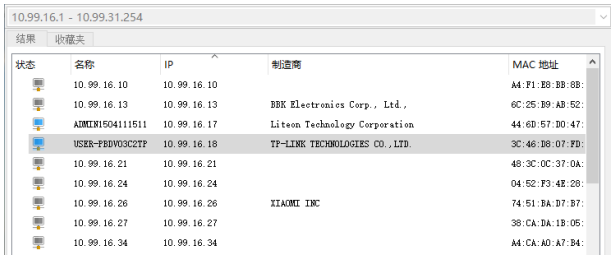

Fig. 3 IP address search

Then the hacker can set up the attack parameters and start the attack operation, the parameters are shown in Fig. 4.

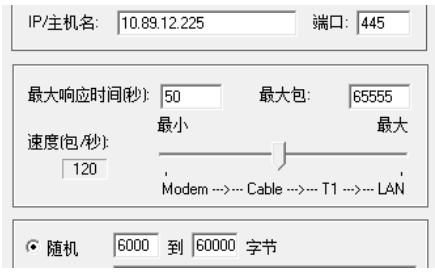

Fig. 4 Attack parameter settings

Fig. 5 shows all packets intercepted on the target host, from which we can clearly see that there are a large amount injection of random data in a certain period of time. As we can see in Fig. 5, a large number of UDP packets and IP packets are crawled, in which IP packets are a warning of the UDP port cache overflow.

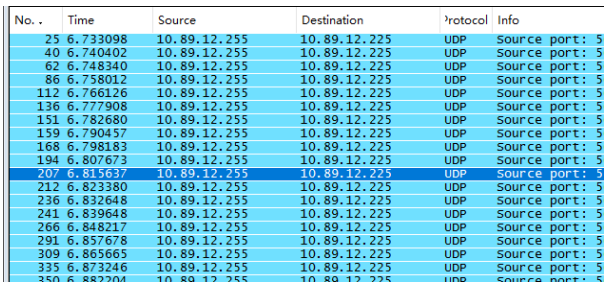

Fig. 5 Attack data validation

By observing the target host, we can find that in a short period of time the data flow increased, and the outflow is reduced, internet speed is greatly reduced, which indicating that the successful attack affects the normal operation of the attacked computer. It also shows that this experiment is feasible for computer terminal using the normal network.

4 Conclusion

More and more malicious cyber attack happened on power systems, and the techniques of attack are more complex, so that the emergency treatment of the security issues is more important than the establishment of a defense measures. The information security issues of SCADA, DCS and other physical information fusion systems and the research about the connection between the network systems will all become the important issues in the future. Improving the defense capabilities of the network and the awareness for protecting the power system of the operators is also urgent. The study of the cyber attack on the power system will occupy an important position in the future power grid construction[26].

References:

[1] Tuballa M L, Abundo M L. A review of the development of Smart Grid technologies [J]. Renewable & Sustainable Energy Reviews (S1364-0321), 2016, 59: 710-725.

[2] Xiang Y, Ding Z, Zhang Y, et al. Power System

https://dc-china-simulation.researchcommons.org/journal/vol29/iss10/35
DOI: 10.16182/j.issn1004731x.joss.201710035

Reliability Evaluation Considering Load Redistribution Attacks [J]. IEEE Transactions on Smart Grid (S1949-3053), 2016 (99): 1.

[3] Wei D, Darie F, Shen L. Application layer security proxy for smart Grid substation automation systems [C]// Innovative Smart Grid Technologies. USA: IEEE, 2013: 1-6.

[4] Peng H, Luo K Y, Tang Z N, et al. Research on power system security defense system in Smart Grid [C]// National Symposium on Conservation and Control, 2011. Nanjing: Chinese society of Electrical Engineering, 2012: 212-218.

[5] Bai D. Smart grid state estimation and performance analysis [D]. Chengdu, China: University of Electronic Science and Technology of China, 2015.

[6] Chen C M, Hsiao H W, Yang P Y, et al. Defending malicious attacks in cyber physical systems [C]// IEEE, International Conference on Cyber-Physical Systems, Networks, and Applications. USA: IEEE, 2013: 13-18.

[7] Pasqualetti F, Dorfler F, Bullo F. Control-Theoretic Methods for Cyberphysical Security: Geometric Principles for Optimal Cross-Layer Resilient Control Systems [J]. Control Systems IEEE (S1066-033), 2015, 35(1): 110-127.

[8] Pasqualetti F, Dörfler F, Bullo F. Attack Detection and Identification in Cyber-Physical Systems [J]. IEEE Transactions on Automatic Control (S0018-9286), 2013, 58(11): 2715-2729.

[9] Liang J, Sankar L, Kosut O. Vulnerability Analysis and Consequences of False Data Injection Attack on Power System State Estimation [J]. IEEE Transactions on Power Systems (S0885-8950), 2015, 31(5): 3864-3872.

[10] Fan L. Analysis of Power System Vulnerability Under Cyber Attack Threat [D]. Beijing: North China Electric Power University, 2015.

[11] Luan H, Lu G. How do the power grid enterprise prevent the cyber attack [J]. China Energy (S1003-2355), 2016 (6): 94-96.

[12] Li Z W, Tong W M, Jin X J. Construction of Cyber Security Defense Hierarchy and Cyber Security Testing System of Smart Grid: Thinking and Enlightenment for Network Attack Events to National Power Grid of Ukraine and Israel [J]. Automation of Electric Power Systems (S1000-1026), 2016, 40(8): 147-151.

[13] Wang W, Zhang D. Analysis of Power System Security and Stability Issues under Electric Market Based on American Large-scale Blackouts [J]. Guizhou Electric Power Technology (S1008-083X), 2014, 17(6): 10-13.

[14] Han L M, Wang L. Research on power system security [J]. Private Technology (S1673-4033), 2015 (12): 52-52.

[15] Tong X Y, Wang X R. Inference and countermeasure presupposition of network attack in incident on Ukrainian power grid [J]. Automation of Electric Power Systems (S1000-1026), 2016, 40(7): 144-148.

[16] Liu N, Yu X H, Zhang J H. Coordinated cyber-attack: inference and thinking of incident on Ukrainian power grid [J]. Automation of Electric Power Systems (S1000-1026), 2016, 40(6): 144-147.

[17] Zhao J H, Liang G Q, Wen F S, et al. Lessons learnt from Ukrainian blackout: protecting power grids against false data injection attacks [J]. Automation of Electric Power Systems (S1000-1026), 2016 (7): 149-151.

[18] Greiman V A. Cyber attacks: the fog of identity [C]// International Conference on Cyber Conflict. USA: IEEE, 2017.

[19] Peter, Fairley. US public utilities' network security system needs to be upgraded [J]. Technology Overview (S2095-4409), 2016 (5): 9-11.

[20] Jing Y F. The study of DoS attack and design of host secure recovery system [D]. Jinan: Shandong University of Science and Technology, 2004.

[21] Liang J, Sankar L, Kosut O. Vulnerability Analysis and Consequences of False Data Injection Attack on Power System State Estimation [J]. IEEE Transactions on Power Systems (S0885-8950), 2015, 31(5): 3864-3872.

[22] Wang L. Application study on vulnerability assessment in power system security defense system [D]. Beijing, China: North China Electric Power University (Beijing), 2005.

[23] Sun B L. Networked control systems and their security issues [J]. Office Automation (S1007-001X), 2011 (4): 45-49.

[24] Zhu J, Zhang G X, Wang T, et al. Overview of Fraudulent Data Attack on Power System State Estimation and Defense Mechanism [J]. Power Grid Technology (S1000-3673), 2016, 40(8): 2406-2415.

[25] Chen-Ching Liu, Jung J,Heydt G T, et al. The Strategic Power Infrastructure Defense System [J]. IEEE Control Systems Magazine (S1066-033X), 2003, 13(8): 40-52.

[26] Sun S, Yan J, Yu Z, et al. Research of power system online dynamic security assessment application expansion [C]// International Conference on Advances in Power System Control, Operation & Management. Hong Kong: IET, 2017.