Security attack detection algorithm for electric power gis system based on mobile application

Chao Zhou¹, Renjun Feng², Liming Wang¹, Wei Huang¹, Yajuan Guo¹

¹State Grid Jiangsu Electric Power Research Institute, Nanjing, 211100, China
²State Grid Suzhou Power Supply Company, Suzhou, 215004, China

Abstract. Electric power GIS is one of the key information technologies to satisfy the power grid construction in China, and widely used in power grid construction planning, weather, and power distribution management. The introduction of electric power GIS based on mobile applications is an effective extension of the geographic information system that has been widely used in the electric power industry. It provides reliable, cheap and sustainable power service for the country. The accurate state estimation is the important conditions to maintain the normal operation of the electric power GIS. Recent research has shown that attackers can inject the complex false data into the power system. The injection attack of this new type of false data (load integrity attack LIA) can successfully bypass the routine detection to achieve the purpose of attack, so that the control center will make a series of wrong decision. Eventually, leading to uneven distribution of power in the grid. In order to ensure the safety of the electric power GIS system based on mobile application, it is very important to analyze the attack mechanism and propose a new type of attack, and to study the corresponding detection method and prevention strategy in the environment of electric power GIS system based on mobile application.

1. Introduction
Geographic Information System (GIS) [2] is widely used as a means of resource management and visual analysis of resources in power generation, transmission, substation, distribution, electricity, communication and other professional. It can effectively improve the data collection, storage efficiency, improve fault location, analysis and processing capacity, and provide support for decision support for the operation of the power grid [3]. At the same time, it can effectively reduce the risk of production and operation. Electric power GIS is a virtual representation of all aspects of electricity, which encompasses all systems including human society, and is expressed in multi-dimensional, multi-scale, multi-temporal, multi-faceted information facilities. So, people can browse, interact, and use a large number of concentrated, power-related elements, such as tower, insulator, substation, etc. With the deepening of the power grid engineering strategy and the deepening understanding of the framework of the electric power GIS system and key technologies, data reception and rapid processing, multi-source heterogeneous spatial data integration, spatial information database, map services and virtual reality and other fields have made corresponding progress

With the development of portable devices, mobile devices are used more and more widely in the daily life and work. In the process of continuous advancement of information technology, the use of mobile terminals to carry out business operations on site has become one of the important work of the
power industry. As a convenient data acquisition and field operations tool, the electric power GIS system based on the mobile application [4] can significantly improve the efficiency of power grid production and management. The introduction of the electric power GIS system based on mobile application is an effective extension of the geographic information system which has been widely used in the power industry.

For now, the power GIS system is not very mature. It carries out the combination and development basically based on the digital earth platform, and then to achieve power production, power management, power engineering and other aspects of the application. Because the openness and sensitivity of the system to the user, it is vulnerable to outside attacks. A new type of false data injection attack [5], which is collecting and analyzing information from a large number of intelligent instruments, can inject the false data into the smart meter to change the information collected by the power SCADA system, and then change the power system state estimation results, to change the load integrity of the power grid. This new type of false data injection attack is also known as load integrity attack (LIA). This type of attack can lead to an erroneous state estimation of the power system, which makes the load distribution unbalanced and further misleads the operation and control functions of the energy management system (EMS) in the electric power GIS system, resulting in catastrophic consequences for the grid. In the face of this kind of load integrity false data injection attack, the current false data detection method is not enough to detect this new type of attack. Therefore, according to the characteristics of the attack, it is imperative to analyze the mechanism of attack and put forward the appropriate countermeasures to improve the operational safety of the electric power GIS.

2. Methods

For the security of social domain strategy: including the staff of the power grid security knowledge and safety skills training, the user safety education for the use of electricity to improve people's awareness of security; the development of safety regulations and policies and regulations to enhance the safety of the power grid Of the system to ensure that; social engineering methods to combat social engineering attacks.

Security protection strategy for information domain: The traditional IT security technology and means can be used to secure the security of intelligent grid information domain, such as encryption and decryption mechanism, secret key management technology can be used to ensure the confidentiality of data, integrity and availability; Access control, authentication and auditing can be used to ensure the normal operation of various services in the smart grid and its security and controllability; IPSec, SSL, TLS, etc. can be in the protocol layer to strengthen the smart grid security; and firewall, intrusion detection, virus check Kill and other technical means can be achieved in a timely manner to detect security threats and its dissemination to suppress, to minimize the destructive.

False data injection attacks belong to a kind of network attack. With the continuous development of attacks, security threats are emerging and evolving continuously. This is essentially an asymmetric technical game between attackers and defenders. Combined with the existing information security defense technology, we use the honeypot technology to break the situation of the false data injection attack and defense asymmetry in order to achieve the purpose of active defense. Honeypot can be defined as a security resource that can be used to capture and analyze attack behavior by deploying some bait hosts or some network service information in the control center to deceive attackers and induce attackers to attack honeypots, and to speculate the attack intentions and motivations. So, the defenders can clearly understand the security threats they face, and then develop technical and management tools to enhance the smart grid system security capabilities.

The basic process of honeypot technology in preventing false data injection attacks is as follows:

1) False data injection attack must first invade the specific host of the control center. The current intrusion detection system can detect the illegal intrusion function. After the detection of the invasion [6], we should start using the redirection function, and let the attack stream redirect to the honeypot host;
2) Because the honeypot host configures the software to imitate the attack, so it is relatively easy to attack, so that it can attract the attacker, and then to dilute the attack and protect the normal host of the control center;

3) Then the attacker will be attracted to attack the honeypot, and the control center host will be replaced by the honeypot system to cut off the control information purposes;

4) The security log function will be deployed in the honeypot system to record different intrusion attacks for learning;

![Figure 1. Honeypot mechanism system diagram](image)

The principal of the use of honeypot technology to prevent false data injection attack is shown in the following figure. The intrusion detection system directs the attack flow to the honeypot. The honeypot system will respond and record the log. Once the intrusion detection system finds that the attacker is in the intrusion control center, the intrusion will be fed back to the corresponding honeypot by address redirection. The honeypot will send an attacker's desired response to the attacker based on the initial setup, making the honeypot think the honeypot is the controlled host, and send control information to the honeypot. Assuming that the probability that the attacker is found by the intrusion detection system and redirects to the honeypot is $P_1$, the number of hosts in a network is $k$, the probability of each host being attacked is $P_2$, and the number of honeypots is $h$, then the probability of successful intrusion to host and the probability of intrusion honeypot are:

$$P_2 \left(1 - P_1\right) k / (h + k)$$  \hspace{1cm} (1)

$$P_1 + \left(1 - P_1\right) h / (k + h)$$  \hspace{1cm} (2)

Analysis of log information can continuously improve the probability $P_1$ that the intrusion detection system finds the attacks, and reduce the probability $P_2$ that the control center host is attacked illegally, to take the initiative to prevent false data injection attack.

3. Results
The simulation results is shown in figure 1 and figure 2.
Figure 2 shows the change in intrusion detection rate with $M$ under the first set of experimental conditions. The results show that with the increase of $M$, the intrusion detection rate is increasing. In particular, when the detection rate of $M_{0.03}/100$ and $N = 1/10$ is 100%, the intrusion detection rate under $N = 1/20$ is more than 97%, and the intrusion detection rate under $N = 1/50$ is more than 75%. That is, when $M = 0.75 / 100$, the experimental results meet all of the test criteria, so to a certain extent, we can say that the spying domain is effective and low cost. Figure 2 also shows that the $M$ value of the spying domain should be set to $0.75 / 100$ because $0.75 / 100$ is the smallest of all $M$ that meets all evaluation criteria.

Figure 3 shows the change in intrusion detection rate with $N$ under different $M$ values.
Figure 3 shows the change in intrusion detection rate with N under the second set of experimental conditions. When \( N = 1/10 \), when \( M = 0.70 / 100 \) and \( M = 0.75 / 100 \), the intrusion detection rate does not all reach 100%. For example, when \( N = 1.1 / 10 \), the detection rates for \( M = 0.70 / 100 \) and \( M = 0.75 / 100 \) are 99.96% and 99.99%, respectively. In contrast, when \( M = 0.80 / 100 \), \( N = 1/10 \) under the intrusion detection rate of 100%, to meet the standard 2. In addition, the attack rate of spyingdomain under \( M = 0.80 / 100 \) satisfies all criteria.

4. Conclusion
In this paper, from the perspective of prevention, we analyzed the measures of the principle of false data injection attack in electric power GIS based on mobile application and the necessary conditions for attack initiation, and put forward the honeypot technology method to protect against attack. Analysis of log information can continuously improve the probability \( P1 \) that the intrusion detection system finds the attacks, and reduce the probability \( P2 \) that the control center host is attacked illegally, to take the initiative to prevent false data injection attack and to ensure the security of the electric power GIS based on mobile application.

This paper opens a new era of deep learning to detect false data injection attacks. In the future, we will carry out relevant work in depth. The intelligent grid load integrity detection and prevention technology still needs to be improved.

Reference
[1] Li H., Lai L., Zhang W. Communication requirement for reliable and secure state estimation and control in smart grid[J]. Smart Grid, IEEE Transactions on. 2011, V2 (3): 476-486
[2] Qiao Shiming. Design and Implementation of Visualization System for Power Network Planning and Design Based on 3D GIS Technology [J]. Science and Technology Innovation Guide. 2015 (02): 118-223
[3] Dan G., Sandberg H. Stealth attacks and protection schemes for state estimators in power systems[A]. Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on[C]. 2010: 214-219
[4] Kosut O., Jia L., Thomas R. J., et al. Limiting False Data Attacks on Power System State Estimation[A]. the 44th Information Sciences and Systems (CISS) Conference[C]. 2010: 1-6
[5] Kosut O., Jia L., Thomas R., et al. Malicious data attacks on the smart grid[J]. Smart Grid, IEEE Transactions on. 2011, V2 (4): 645-658
[6] Yuan Y., Li Z., Ren K. Quantitative Analysis of Load Redistribution Attacks in Power Systems[J]. Parallel and Distributed Systems, IEEE Transactions on. 2012, V23(9): 1731-1738