http://www.inosr.net/inosr-applied-sciences/
Kalulu
INOSR APPLIED SCIENCES 9(1):9-12, 2022.

International Network Organization for Scientific Research ISSN: 2705-165X

The Smart Grid and Its Security Challenges

Kalulu Mathias

Department of Electrical, Telecommunications and Computer Engineering, School of Engineering and Applied Sciences.

ABSTRACT

Since its birth over a century ago, the power system in the United States has been evolved into one of the largest complex networks ever witnessed in human history. With the increasing consumption demand, the modern electrical power grids are now growing into a mammoth system with numerous interconnected regional grids, owned and operated by power corporations at all levels and scales. However, complex interests, operations and managements among different power companies often complicate cross-region transmission tasks and sometimes result in an inefficient or poorly-coordinated power delivery. And the traditional power grids in modern times are facing some rising challenges. As the need and variety of consumption increases, more and more latest technologies have been incorporated into the power system, such as the distributed renewable energy generation, the electric vehicle (EV) charging system, smart meters, etc., which all contribute to the complexity of modern power delivery. The ever increasing reliance on electricity and request of power quality have been constantly calling for better power delivery, more flexible pricing, faster power restoration, among others. The challenges above have motivated the industry and society for a new generation of power system with more informative, intelligent and automatic operations.
Keywords: Smart Grid, Security Challenges and power

INTRODUCTION

This new generation of power grid, commonly referred to as the Smart Grid, will modernize the traditional power grid and improve its reliability, flexibility and efficiency. The Smart Grid is expected to have more distributed controls and consumer-based interactions, and some key applications of this upgrade include Installing advanced metering infrastructure (AMI) and other intelligent de- vices to reduce extra unnecessary demand, as well as the operation and main- tenancy cost, implementing distributed automation to enhance the reliability of power sys- term and utilizing automated controls for better and flexible power management The most significant feature of the Smart Grid, in contrast to the traditional power system, is the large scale of implementation of a two-way communication network connecting both the power plants, the transmission network sensors and the consumers. This enhanced and interactive system will optimize the power delivery quality, efficiency and stability at a lower cost via the computer-based automation. With the incorporation of communication and computer networks in assistance to the traditional power delivery, the Smart Grid is already an emerging gigantic intelligent network system in which power flows are flexibly directed by highly automatic systems like the Supervisory Control and Data Acquisition (SCADA) system. However, the Smart Grid yields not only a boost of economic benefits but also a growing number of potential threats from the cyberspace [6]. While the distributed control can reduce the criticality of some control centre and thus weaken the impact of attacks targeted on them, the distributed access from the system-on- a-chip (SoC) electrical devices can possibly allow malicious attackers penetrating into the power systems with increased difficulties to detect and track them. Mean- while, with the huge volume of data

flowing along the power transmission network, they are becoming more vulnerable to data or command interception and unauthorized modification, which can be utilized to either cheat the meters for an unfair price or disrupt power system operations. More seriously, knowledge of the power Grid can be learned and the information or intelligence could be used to hack into the distributed control units that may be less protected than the centralized operation and management hubs, resulting in unpredictable security risks. Hence, it becomes crucial to realize and react to the vulnerability of Smart Grid in the new forms of potential attacks. These "smart" attacks, if deliberately designed and launched successfully on some critical components, can cast a disastrous impact on the power grid transmission and significantly jeopardize the interest of both the public, the industry as well as the economics. The traditional power grids have transformed into smart grids by the rapid integration of technologies. According to [1]. Smart Grids is a concept regarding digital technology application and electric power network. Smart Grid includes electric network, digital control appliance, and intelligent monitoring system. All of these, can deliver electricity from producers to consumers, control energy flow, reduce the loss of what, and make the performance of the electric network more reliable and controllable [1].

Neural network

A neural network is either a system software or hardware that works similar to the tasks performed by neurons of human brain. Neural networks include various technologies like deep learning, and machine learning as a part of Artificial Intelligence (AI) ViRealtime monitoring and control of the smart grids are ascertained through AMI. The AMI infrastructure has revolutionised the management and development of power systems by providing newer means of data exchange. Advanced Metering Infrastructure is a network of devices that record, store, and transmit the energy usage data. It provides a suitable link between the end users and electric power utility. The AMI is an upgrade of Advanced Meter Reading (AMR) system, where smart meters play the most important role in collecting data.,[2].

Smart Grid Security Analysis

While the blooming Smart Grid technologies, the security issues are also becoming more challenging with the mass computer based monitoring, control and metering, and numerous researches have proposed their general frameworks or plat- forms from their perspective for the comprehensive understanding of smart grid security. In this section, we will discuss the general security issues and the major types of Smart Grid attacks, with some powerful tools developed to assess and address these issues.

Smart Grid Security Issues

Smart Grid, as an integration of power transmission networks and commune-action networks, can be vulnerable in both physical and cyber space. These include challenges in accurate measurement and monitoring of power system states, power transmission reliability against disruptive events, control of access and authentication, detection and defence against malicious attacks, as well as the protection of user privacy. Coordinated attacks can take place in both networks and it can be difficult to identify these attacks and distinguish them from usual disturbances, especially when millions of users data are also recorded by smart meters all across the country, while there are only a few control centres to ensure the stability of the whole interconnected systems. In this thesis, we are specifically interested in the attacks on power system directly, which usually bring the most catastrophic effects if proper counter-measures are not called in time. However, in reality attacks on different levels can be launched simultaneously, so we will first briefly explore the major types of Smart Grid attacks to better explain the related fields for this study.

Categories of Smart Grid Attacks

Generally, to refine the scope of the thesis we can roughly divide attacks in the Smart Grid into three categories based

on the definition in [3], which are the consumer-end attacks, the data attacks, and the direct attacks, and the subject of this study will be the last type that can lead to the most severe impact to the power system.

Consumer-end Attacks

The consumer-end attacks are the attacks happening at the consumer end, e.g. Smart meters or distribution network controllers. Many of these at- tacks are the personal attempts to treat the meters with some software or Trojan scripts for unfair electricity price, or to steal user consumption profile for private information. Although they do not carry the purpose to jeopardize power system stability or security which appears less fatal or impactful, consumer-end attacks is not trivial as the user-end devices have feedback access all the way up to control centers. If attackers aim at creating social chaos, they can still try to forge suspicious or erroneous requests and send them to the control center, resulting in a denial of power delivery service for the "corrupted user demand". This denial may either shut down the switch of normal residential buildings or interrupt the quality of power delivered to critical social infrastructures like hospitals, transportation. In other cases, user data can also be stolen from the smart meters, giving off private information that can pose other threats to individual users. To address issues raised by this type of attack, researchers have been focused on the development of a secure interaction between the smart meter and the users. These include better encryption and authentication,as well as advanced meter reading and communication techniques In addition, privacy issues have also been studied from both hardware and software aspects.

Data Attacks

By its name, data attacks are the type of Smart Grid attacks targeting at the data flow that are transmitted along the communication network Many researchers suggest that the data attacks are mostly related to the state estimation of power systems Attacks of this type include insertion, alteration, or deletion of data or control commands The application of these attacks can overlap with the consumer-end attacks in the deception of metering devices, but usually in data attacks they are targeted at power system instead of a single user-end device and organized in a more specialized way. As some studies have revealed, the detection on the false data injection or load alteration attacks can be very difficult if the attackers have sufficient knowledge about the topological information of the power grids. In these worst cases, the attackers do not have to know about the operating point or the exact states of the system, yet they can nevertheless forge fake data without showing anomaly and successfully walk around the traditional detection methods. Because of the data protection can be extremely hard due to the vast amount of data collected and generated through a gigantic network, there are still many ongoing researches to optimize the chance of detection and lower the risk of disastrous consequences from data attacks.

Direct Attacks

The most severe attacks in the power grids is the cyber-physical ones directly aimed at the disruption of critical power transmission network components like power plants, substations or transmission lines. By creating outage and tripping of these components which were in normal operation, the attackers can turn an interconnected power system into an instable state, which usually ends up in massive blackouts as a consequence of cascading failures. In reality, direct attacks can be done by via data attacks, for instance forging fake messages of system state, outage, instability or tripping and sending them to the control centers, resulting in mistaken actions and regulations that causes cascading effects. These attacks can also be coordinated in a cyber-physical space by tools like Petri-nets [4], which will significantly increase their chance of success and the severity of the attack. Studies have shown that by exploiting the vulnerability of power systems, direct attacks can be studied as contingencies of outage since they have

similar effects, yet the consequence of these malicious attacks can be much more catastrophic with the well-chosen victims selected by the intelligence information.

Smart Grid Security Tools

To address the security issues, many traditional approaches from the net-work security studies, including intelligent and efficient trust control, advanced encryption, bad data detection, etc. Have been introduced. In addition, to better approximate and understand the interaction between attackers and defenders in securing the Smart Grid, theorems and techniques from game theory, petri-net, clustering/partitioning, data mining have been introduced. Researches based on game theory can effective display the optimal choice for both attackers and defend errs based on their own cost in the scenarios Petri-nets are very powerful in identifying and handling multiple events happened cyber-physically Clustering and partitioning techniques reveal critical and effective measures to refine the influence of attacks with a small area so that the protection and restoration will cost significantly less. Data mining algorithms can take great advantage of the growing volume of data collected throughout the Smart Grid network sensors and extract important information on the healthiness and anomaly of the opera- tin power grids. Still, many of these tools are facing difficulties in application due to their scalability, computational efficiency or real-time capabilities.

CONCLUSION

AMI in the grids is very important part, which is always a target of cyber criminals for various purposes including energy theft. The cyber defence for AMI to detect and prevent these vulnerabilities is always a challenging task.

REFERENCES

1. Zhu, S., Lee, J. S., Guo, F., Shin, J., Perez-Atayde, A. R., Kutok, J. L., Rodig, S. J., Neuberg, D. S., Helman, D., Feng, H., Stewart, R.A., Wang, W., George, R.E., Kanki, J.P., and Look, A.T. (2012) Activated ALK Collaborates with MYCN in Neuroblastoma Pathogenesis. Cancer Cell. 21(3):362-373.
2. Gregory, S., Barlow, K., McLay, K. (2006). The DNA sequence and biological annotation of human chromosome 1. *Nature* **443**, 1013.
3. Mohammed, H., Tonyali, S., Rabieh, K., Mahmoud, M. and Akkaya, K. (2016). Efficient privacy-preserving data collection scheme for smart grid AMI networks," in GLOBECOM. IEEE, pp. 1–6.
4. Jokar, P., Arianpoo, N. and Leung, V. C. (2015). Electricity theft detection in AMI using customers' consumption patterns. IEEE Transactions on Smart Grid, 7(1), pp.216-226.
5. Masisani William Mufana and Adabara Ibrahim (2022). Monitoring with Communication Technologies of the Smart Grid. *IDOSR Journal of Applied Sciences* 7(1) 102-112.
6. Nabiryo Patience and Itodo Anthony Ejeh (2022). Design and Implementation of Base Station Temperature Monitoring System Using Raspberry Pi. *IDOSR Journal of Science and Technology* 7(1):53-66.
7. Masisani William Mufana and Adabara Ibrahim (2022). Implementation of Smart Grid Decision Support Systems. *IDOSR Journal of Scientific Research* 7(1) 50-57, 2022.
8. Natumanya Akimu (2022). Design and Construction of an Automatic Load Monitoring System on a Transformer in Power Distribution Networks. *IDOSR Journal of Scientific Research* 7(1) 58-76, 2022.
9. Kisakye Rebecca (2022).Simulation and Analysis of Dipole Transmitter Antenna (KIU Laboratory) *IDOSR Journal Of Computer And Applied Sciences* 7(1):119-135.