Security of State Estimation in the Smart Grid

Wei Fan, weifan (at) wustl.edu (A paper written under the guidance of Prof. Raj Jain) Download

Abstract:

The power system is one of the most critical national infrastructures, the security and stability of which is the foundation of social stability and plays a key role on the fast and healthy development of the national economy. As a core module of the online security analysis system, power system state estimation is a major part of modern energy management system.

This paper describes the security risks, security objectives and security research trends in smart grid technology. We introduce the fault detection and bad values of traditional power system state estimation methods, and then further describe false data injection attacks.

Keywords: Smart Grid, State Estimation, SCADA, False Data Injection Attack, Power System, Security

Table of Contents:

---

1 Introduction

A traditional electric power system includes generation, transmission, transformation, distribution and utilization. With the rapid development of society, peopleâ€™s demand on the systems has increased, which means the traditional power system will be unable to meet the growing demand for electricity. In this case, the smart grid emerges at the right moment.

The smart grid, as the next generation power grid system, which needs to integrate a variety of renewable energy resources, also needs to integrate a high-speed, reliable and secure data communications networks and intelligent data processing center to deal with increasingly complex grid system, and provide efficient and intelligent management. More precisely, the smart grid

is a new type of electric power system. It integrates two-way, secure information and communication technologies and computational intelligence with the generation, transmission, transformation, distribution, utilization and all aspects of electricity, in order to build a clean, reliable, flexible, efficient, sustainable and safe power system.[1]

A traditional electric power system transfers the power that is generated by central power generators to many users and consumers. In contrast, the smart grid uses a two-way flow of information to create a high level of automation and a distributed energy delivery network. Table 1 gives a simple comparison of the existing grid and smart grid.

Table 1: A simple comparison of traditional grid and smart grid

Traditional grid	Smart grid
Electric machinery	Digital
One-way communication	Two-way communication
Centralized power generation	Distributed power Generation
A small number of sensors	Full grid sensor layout
Manual monitoring	Automatic monitoring
Manual recovery	Automatic recovery
Failures and power outages	Adaptive and Islanded
Few user options	More user options

Smart grid is an important step in the electric power system in order to meet the new needs of today's users who have appeared and possible users in the future. The development of smart grid power system brings many new fine features. At the same time, it introduces some new security issues to the power grid, which makes it vulnerable to potential network attacks.

To ensure the safety and the reliability of the power system, the control center electric power system uses an industrial data acquisition and the control system, named Supervisory Control And Data Acquisition (SCADA) system, for monitoring and control of each interconnected component in the electric power system. The SCADA system, obtains the information of the power systemâ€™s status every 2-4 seconds[2] by reading the power measuring instruments erected on the key components. What the measuring instruments measure include busbar voltage, busbar active and reactive power injection and reactive flow for each subsystem. These measurements are transmitted to the control center, and the staffs in the control center collect important system data and provide centralized monitoring and control capabilities for the power system with the aid of computers.

The state estimation of electric power system is an essential function for system monitoring, which is an important part of modern energy management system (EMS). The state estimation of electric power system uses the redundancy of measurement data provided by SCADA to improve the accuracy of data, automatically exclude error messages caused by random interference, and estimate or forecast the running state of the system. It makes the optimal power system state estimation through the measurements of instruments and analysis of power system models. Staffs in the control center use the outputs of the state estimation process as the base for accident analysis. In the accident analysis, they judge potential operational problems, and give out operational guidance to avoid these problems, as well as possible side effects caused by these actions.

Because SCADA plays a crucial role in the state estimation of the electric power system, which provides the source of data, becomes one of the most vulnerable targets for attack. Theoretically, Liu Y.[3] proposed false data injection attacks from an attackerâ€™s perspective, which aims at the state estimation of electric power system. This method consists of systematically tampering with the measurement data of meters, bypassing the traditional error data monitoring, then successfully influencing the state estimation. Also, literature [4][5] did a research on the impact of false data injection attacks to the real-time electricity market. This kind of attack can achieve improper financial profit by influencing the marginal price of nodes in the electricity market, which provides sufficient motivation for attackers.

2 Introduction of smart grid security issues

With the introduction of excellent new features and diverse functions into the smart grid system, and more cooperation over the network, the security issues of smart power systems deserve further attention.

2.1 Security risk of the smart grid

The smart grid technology will allow the current electricity system to add new functions and features. However, it will also bring new security risks to the electric power system. We rely on the power supply system, and this kind of strong dependence on the power system also make the power system a crucial property and indispensable critical infrastructure to support social functioning. Interruption of the electrical energy supply would bring enormous social impact. The security of the power system is an important issue. The security risks introduced by the smart grid are related to its communication needs, system automation, new technology and the data collection[6].

The smart gridâ€™s backbone is its computer network, which connect different components to a smart grid, and provide it with a two-way communications. Networked components would bring more security risks to the system. However, this is required for the smart grid to achieve many of the major functions. Meanwhile, the networked components also increase the complexity of power system, which brings more opportunities to security vulnerabilities. In addition, the networked component also makes more entities can access the electric power system.

The smart grid uses a computer network to transmit data, and uses software to automate the maintenance of electrical systems. Data transmission systems that rely on computer networks can introduce security risks. Some components require real-time data, and communication delay or loss of data may endanger the electric power system. Related management software of the power system will also face the risk of malicious code. Communication or system status management software interrupts may cause energy loss, and in extreme cases may also cause casualties. Different networked components in power system require interoperability between different technologies, and this process will also introduce security risks. Taking the size and cost of electric power systems into account, the legacy systems cannot be replaced in a short period. In this case, the new smart grid systems must be compatible with legacy systems. However, the legacy systems did not implement new security features that modern systems have, and the legacy grid systems will be the weakness of smart grid safety. In addition, the new technology used in the smart grid may also have some hidden security vulnerabilities to explore.

It is estimated that the amount of data in smart grid will increase an order of magnitude. A substantial increase in the amount of data will bring the problems of privacy and security. Also, smart grid will also collect some new types of data, which may also lead to privacy problems.

2.2 Security goals of the smart grid

The security objectives of smart grid are different from other industrial products. One of the most important things is that any security measures implementation should not impede the availability and safety of power use. For example, locking the system after several failed passcode attempts cannot be used in a smart grid system, because locking the power system may lead to security personnel problems in emergency situations. Typically, the importance of security objectives is in the order of confidentiality, integrity and availability. For most industrial products, confidentiality and integrity are more important than availability. But in the electric power system, we must keep the power always available, which means the availability is the first one, then the integrity, and then confidentiality.

Availability is the most important security goal in electric power system. It is estimated that the maximum delay that the critical real-time smart grid system can tolerate is 4 milliseconds. Any interruption of monitoring or communication in smart grid system can result in energy losses. Table 2 lists the approximate maximum communication delay requirements[6]. Availability is not only the most important goal for the power system, but also a crucial objective for the majority of components in the power system.

Table 2: Maximum communication delay requirements

The maximum delay	Communication type
≤4 Millisecond	Relays protection
Subsecond	Wide area status monitoring
Second	Substation and branch monitoring and SCADA
Minute	Non-critical equipment and market price information monitoring
hour	Meter reading and long-term price information
≥day	Long-term use of the data collected

The importance of integrity in smart grid is behind availability. The smart grid gathers data from agency or by using various sensors. Then it uses the original data with the estimation of power system state, to monitor the current state of electric power system. The integrity of this data is very important. Unauthorized data modification, or inserting data from an unknown source, will result in errors or even destroy of the electric power system. Power supply systems not only need to be available in any time, but also require a high quality. The power quality assurance is also dependent on the state estimation of th power system. The quality of estimation depends on many factors, while data integrity is one of the most important factors.

The third objective of an electric power system security is confidentiality. For a smart grid, the cost of confidentiality loss is smaller than loss of availability or integrity. Of course, in some domains of smart grid application, the requirements of confidentiality will be higher, such as personal user information, company information and electric power marked information.

3 Power system state estimation

Power system state estimation is one of the most important parts of EMS in modern power system. It builds the core modules of electric power system online security features analysis. It is like a filter set up between the original data and all applications that need to use the data of current system state.

Power system state estimation using a SCADA system to provide measurement data redundancy to improve data accuracy, automatically exclude from the error message caused by random interference, and estimate or forecast the running state of systems.

3.1 Power system operating state

At a given time point, if the network model of the power system and each busbar voltage vector is known, then the operating state of the power system can be determined. Since the voltage vector sets can be described completely, it is called the static state in electric power system. According to the literature[7], with changes in the operating state, the system might enter the following three states: the normal state, the emergency state, and the restorative state.

If all loads under the system obtain electric power supply without violating any operating restrictions, then we say the electric power system in a normal state. Operating restrictions includes the limit of transfer current and the minimum and maximum busbar voltage limits. If a system is under the normal state, after any accident that list in the event prevention table, the system can still maintain a normal state, then we say that this normal state is safe. General accidents include equipment failures and

transmission line failure caused by bad weather. On the other hand, if all the operations of system are restricted without cross-border, but the system is still sensitive to some accident that is within some scopes of consideration, then we say that such a status is not safe. If the status of a system is normal but not safe, then some actions should be taken immediately to prevent the system transfer into the emergency state. Such preventive control can be determined with the help of optimal security restrictions programs.

Due to an unexpected event, the operating state may change drastically, which can lead violation of operating restriction, in the case of continuous electric power supply. In such a case, we say that the electric power system is under the emergency state, which needs the operator to take corrective action urgently to make the system back to normal state.

When the system is in a state of emergency, the corrected control operations can reduce various loads, lines, transformers and other equipment in order to avoid a system crash. In that case, the violation of operation restrictions is eliminated. The system will recover stability by cutting down loads and reconfiguring the topology. Besides, in order to supply power to all loads, those loads that break the balance of power loads will also be recovered. This state of operation is called the restorative state. The operation that returns the system to the normal state is called control recovery. Figure 1 illustrates the possible conversion process between the states defined above.

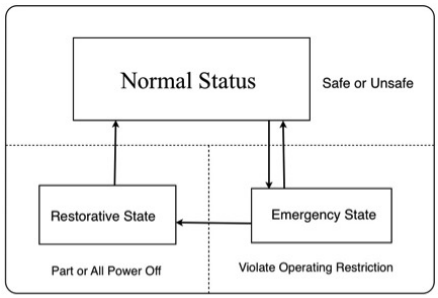

Figure 1 Power system operating state transformation diagram

3.2 Power system security analysis

The operators in control center control the electric power systems. The main tasks for these operators are maintaining the normal and safety state under different daily operation.

To achieve this goal, continuous monitoring of system status and state of operation are required. Necessary protective measures must also be determined for when the system is in a not safe state. This sequence of operations is called a security analysis of the system.

The first step of security analysis is monitoring the current state of system. This process uses measurement values throughout the whole system, and processes this data to determine the state of system. The measured values can be either analog or digital. Substations are equipped with remote terminal units (RTU). An RTU is responsible for collecting various types of measurements and transferring these data back to the control center. However, in the current case, the intelligent electronic devices (IED) are gradually complementing and replacing the RTU devices. It is possible to form a LAN by connecting SCADA systems and other equipment. SCADA system helps transmitting the collected data to the SCADA host that placed in control center. The host in control center collect data through all possible communication links, such as optical fiber, satellite, microwave and so on. Figure 2 shows a typical system configuration of EMS/SCADA system.

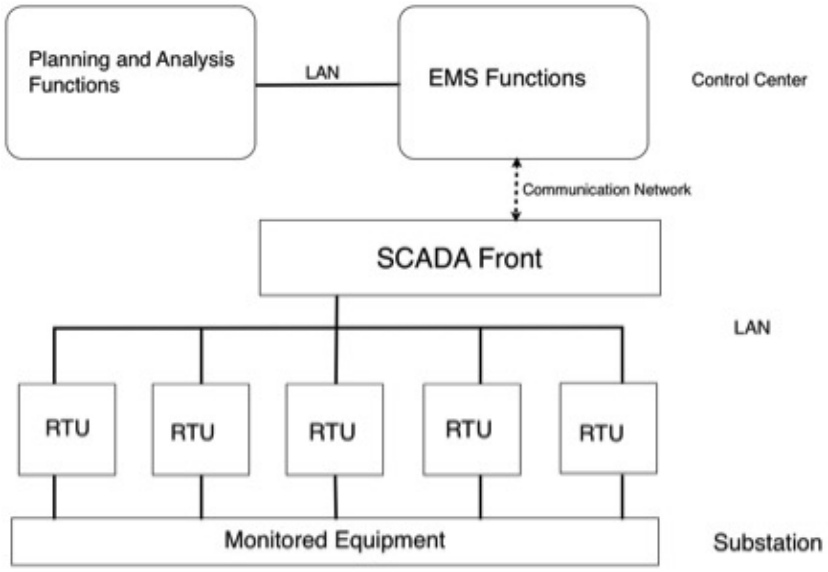

Figure 2 EMS / SCADA system configuration

The measured values that are received by control center including line flow, busbar voltage, the generator output, load, and line switch status. These original data and measurement values are processed by the state estimator to filter out measurement noise and detect serious errors. In the available measurements and system modeling assumptions, the state estimator will give the optimal solutions of power system state estimation. Then, the optimal estimate will be delivered to all EMS applications, such as fault analysis, automatic generation control, and load forecasting and flow optimization. Also, the same information can be connected to the corporate office through LAN access. In the office, other analysis functions can be done offline.

Initially, the electric power system is only monitored and controlled by remote system. Those systems are essentially monitoring and controlling the circuit in substations. In order to cooperate with applications such as Automatic Generation Control (AGC) and Economic Dispatch (ED), the measurement of generator output power and system frequency are also required. Gradually, those remote control systems strengthen to have real-time data acquisition capabilities, so that the control center can collect a variety of measurements data and switch status of circuit from the power system. However, the data provided by the SCADA system, thanks to the presence of measurement noise, communication error, and the telemetry noise, is not always reliable. Besides, the measured values that are collected cannot directly provide the operation states.

3.3 Power system state estimation

Above problems first raised by Fred Schweppe, and he also first proposed power system state estimation [8,9,10]. The introduction of state estimation function broad the ability of the SCADA system, and also makes the EMS system to be constructed. EMS system will be equipped with an online state estimator.

In order to identify the current operating state of electric power system, the state estimator monitors the operational restriction in an accurate and efficient way with the help of the load on transmission line and voltage of busbar. They provide reliable and real-time database for the power system, including safety assessment modules and data to analysis.

State estimator typically includes the following functions:

- Topology Processing: collect the status of circuit breakers and switches, and configure the systemâ€™s online diagram form.
- Observability analysis: determine whether the existing measurements value is adequate to estimate the entire power systemâ€™s state and solutions. Also, recognize unobserved branch and observability island in system.
- Estimate solution: Based on the network model and system measurements that collected, determine the optimal estimation of the entire system. Also, it will provide all the linesâ€™ flow, loads, generator output and transformer taps

optimal estimation.

- Bad value processing: detect the presence of significant errors of measurement values. Identify and remove bad measurement values under the conditions with sufficient redundancy.
- Number errors and structures errors processing: Estimate the various network parameters such as transmission line model parameters.
- Network parameters estimation: estimate various network parameters, such as transmission line model parameters, tap changing transformer parameters, bypass capacitors and reactors parameters. Detect errors of network configuration results, and identify errors in the measured value with sufficient redundancy.

Therefore, the power system state estimator built the core module of online security analysis. It is set up like a filter between the original data and the applications that need to use those reliable data. Figure 3 describes the data state estimator and online static security assessment process, in which involves a variety of applications and functional interface.

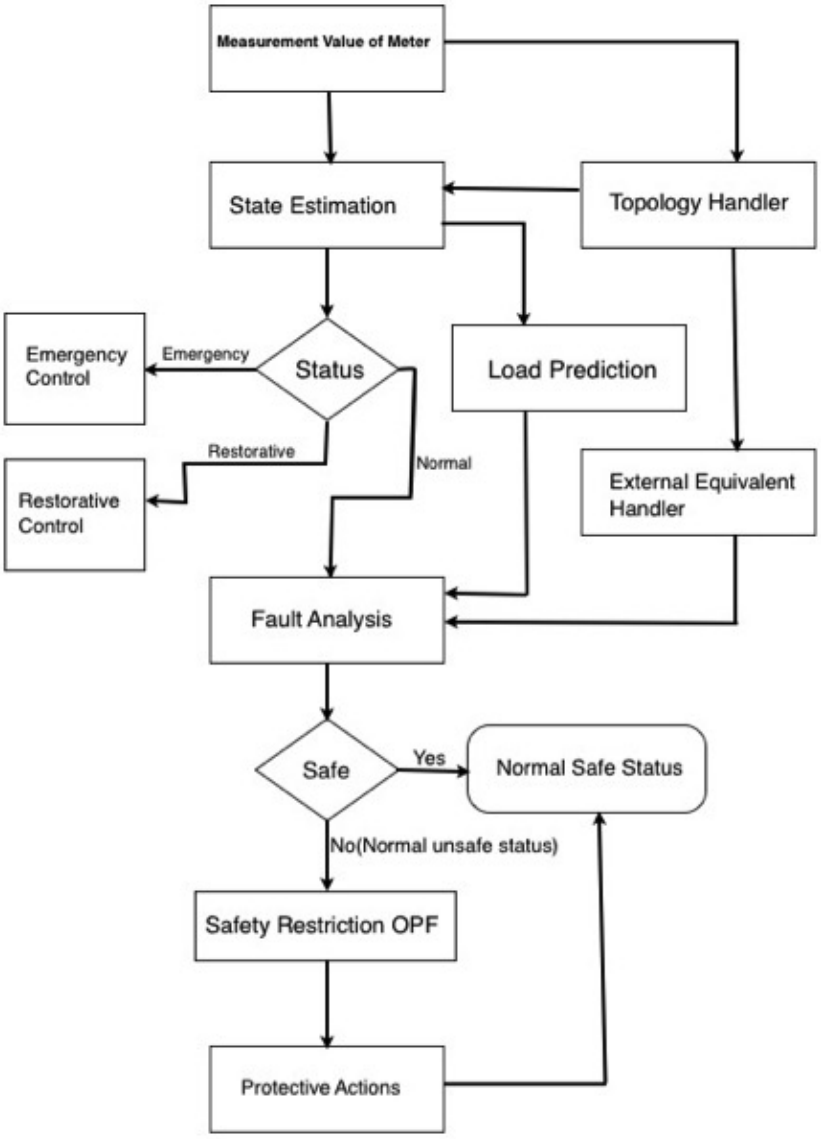

Figure 3 Line static security assessment capabilities schematic

3.4 State Estimation bad value detection defects

In the power system state estimation process, it is conceivable that the attackers could achieve a certain goal by injecting

malicious measurements. For example, an attacker can directly invade meter substations or stored meter measurements to inject malicious data. If these bad measurements affect the status of the estimated output, then the error message generated will mislead the control center, helping the attacker to further achieve their goals.

Researchers have realized the threat of bad measurements in power systems and studied the relevant processing methods[1,2,11,12]. These methods are the first monitor whether the data is bad, and then try to identify and remove those bad data.

However, Liu[3] pointed out that if an attacker knows the current configuration of the power system, and the value of all existing detection algorithms based on bad direct current (DC) models have similar defects, an attacker can bypass their protection. The basic reason is that all the available models based on DC measurement value detection and identification of bad algorithms are based on the assumption that the difference between the measured value "occurs when bad measurements, the observed and their corresponding estimate of square is great." The literature[3] gives proof that this assumption is not always true. From the attackerâ€™s point of view, false data injection attacks can be made, which can bypass traditional bad value detection algorithms.

4 False data injection attacks

False data injection attacks is one of the most common form of attacking for the smart grid systems. In this chapter we will discuss the principle, requirements and scenario of false data injection attacks.

4.1 DC state estimation and bad value detection

In order to ensure the continued operation of the power system, even if some components of error, electrical engineers use the meter to monitor system components. These meters will measure the active power flow in the power system and branch active power injection of each busbar, and the measured value will be submitted to the control center, which will control center use the measurement value to estimate the state variables. State variables include busbar voltage phase angle and amplitude (in DC load flow model, the voltage amplitude and reactive power flow is usually unnecessary to consider, so the state variables are usually only voltage phase angles). After obtaining the estimated values of the state variables, the control center determines whether the entire system is in normal state. In a word, the problem of state estimation is to use the measurement value to estimate state variables of electric power system.

More precise definition is as follows. Use $\mathbf{x}=(x_1,x_2,â€¦,x_n)^T$ and $\mathbf{z}=(z_1,z_2,â€¦,z_m)^T$ to denote the state variables and measured values, n is the number of state variables, m is the number of measured values, and mâ‰¥n. Use $\mathbf{e}=(e_1,e_2,â€¦,e_m)^T$ to denote measurement error. State variables and the measured value linked via $\mathbf{z}=\mathbf{h(x)}+\mathbf{e}$.[13]. Typically, the number of meters is far more than the number of state variables. Thus, overdetermined linear equations with m equations and n unknown number will result. Taking into account the existence of the error, the overdetermined linear equations cannot be solved. The following three methods are usually used in state estimation: maximum likelihood estimation, the weighted least squares estimation, and the minimum variance estimation [14]. When the measurement values obey normal distribution with mean zero, the above three criteria will export same optimal estimation results.

Due to various reasons, such as the meter error and malicious attacks will introduce bad measurements values. There have been many studies on the bad value detection technology to protect state estimation[14,15]. Intuitively, the normal measurement meter typically generates a value close to the actual state variable. If the state estimator thinks there might be a bad measurement value, it will issue an alert.

4.2 The principle of false data injection attacks

Suppose there are m meters providing m measurements values: $z_1,z_2,â€¦,z_m$, and electric power system with n state variables: $x_1,x_2,â€¦,x_n$. The relationship between the m measurement values and n state variables represent as an **MÃ—N**

matrix **H**. In general, **H** matrix is determined by the power system topology and line impedance of the power system. How to build **H** matrix have been explained in literature[15]. Assuming an attacker can access the **H** matrix of target power system, and can manipulate a certain number of measurement value of meters. Then the attacker can modify the measurement values systematically, and bypass the bad value detection algorithm, and affect the optimal estimation value of electric power system by injecting bad data.

$\mathbf{Z_a}$ indicates the measurement value matrix containing malicious data, which can be expressed as $\mathbf{Z_a}=\mathbf{z}+\mathbf{a}$. In which $\mathbf{z}=(z_1,z_2,â€¦,z_m)^T$ denotes the original measurement vector, $\mathbf{a}=(a_1,a_2,â€¦,a_m)^T$ is the malicious data added to the original measurement value, also known as attack vectors. An attacker can choose any non-zero vector as an attack vector a, then construct a malicious measurement value as $\mathbf{Z_a}=\mathbf{z}+\mathbf{a}$. If the attack vector is a linear combination of matrix **H**, then it can pass the traditional bad value detection. This kind of attack is called unobservable attack, or false data injection attack.

4.3 Requirements and the actual meaning of the attack

To achieve the false data injection attacks, the there are a lot of things that attackers need to do.

First, the attacker must know the current configuration of the target electric power system, in particular the topology of the system. The power systemâ€™s configuration changes frequently because of the planned and unexpected maintenance. Typically, this information is only accessible for control center. Taking the sensitivity of the control center into account, the physical access of the control center is highly regulated and protected. Therefore, it is very difficult for an attacker to obtain configuration information to launch the attack.

Second, the attacker must be able to manipulate a certain number of measurement values. An attacker would need to physically tamper the meter or modify the measurement values before they are transmitted to the control center. However, in most cases, meters are in a place with protection against unauthorized access, such as substations. Therefore, it is not easy to manipulate these meters.

The key benefit for studying false data injection attacks is to expose the weakness of the existing state estimation techniques. The exact impact of the attack is not only dependent on the introduction of errors, but also on how to use these measurement values. In one particular application in today's power system, staff in control centers usually need to join the decision-making process. Experienced operators may be able to identify anomalies caused by this attack. In order to clarify these attacksâ€™ meanings in different scenarios, more research will be necessary.

4.4 Attack scenario

Literature[16] considered two possible targets, which are random false data injection attack and purposeful false data injection attacks. In random false data injection attack, the purpose of attacker is to find any attack vectors that can cause miscalculation of the state estimation. In purposeful false data injection attacks, attacker tries to inject specific errors to a particular state variable. The former attack is easier to achieve, while the latter may cause a greater hazard.

Besides, literature[3] also mentioned the following two possible attack scenarios, and discuss attackers how to find the attack vectors and launch unobservable attacks. Scenario 1 is for limited access to meters. In this scenario, the attacker can only access some limited and specific measurement meter. The cause of this phenomenon may be the existence of different physical protection of the meter, such as some meters are inside substation and under great monitoring, while others are outside and only protected with an iron box. Scenario 2 is for limited resources available. In this case, attackersâ€™ resources only enough to access limited number of meters. So attackers will try to find the attack vector with minimum cost.

5 Summary

The power system is one of the most critical national infrastructures, the security and stability of which is the foundation of social stability and plays a key role on the fast and healthy development of national economy. As a core module of the online

security analysis system, power system state estimation is a major part of a modern energy management system. This paper describes the security risks, security objectives and security research trends in smart grid. We introduce the fault detection and bad values of traditional power system state estimation method, and then further describes the false data injection attacks.

According to what is mentioned above, erroneous data injection attacks can be achieved by taking advantage of the shortcomings of traditional bad value detection algorithms. This paper analyzes the basic principle of this attack, the attack conditions and scenarios. However, we did not discuss how to prevent this kind of attack, although some researches indicate that this problem might be solved by the deployment of phasor measurement unit (PMU)[17]. Thus, what we can do in the future is to find some appropriate way to prevent the false data injection attack, as well as more advanced attack methods.

6 Reference

1. Fang X, Misra S, Xue G, et al. Smart gridâ€"The new and improved power grid: A survey[J]. Communications Surveys & Tutorials, IEEE, 2012, 14(4): 944-980.
2. Bobba R B, Rogers K M, Wang Q, et al. Detecting false data injection attacks on dc state estimation[C]//Preprints of the First Workshop on Secure Control Systems, CPSWEEK. 2010, 2010.
3. Liu Y, Ning P, Reiter M K. False data injection attacks against state estimation in electric power grids[J]. ACM Transactions on Information and System Security (TISSEC), 2011, 14(1): 13.
4. Xie L, Mo Y, Sinopoli B. False data injection attacks in electricity markets[C]//Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on. IEEE, 2010: 226-231.
5. Jia L, Thomas R J, Tong L. Malicious data attack on real-time electricity market[C]//Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on. IEEE, 2011: 5952-5955.
6. Metke A R, Ekl R L. Security technology for smart grid networks[J]. Smart Grid, IEEE Transactions on, 2010, 1(1): 99-107.
7. Liacco T E D. Real-time computer control of power systems[J]. Proceedings of the IEEE, 1974, 62(7): 884-891.
8. Schweppe F C, Rom D B. Power system static-state estimation, Part II: Approximate model[J]. power apparatus and systems, ieee transactions on, 1970 (1): 125-130.
9. Schweppe F C, Rom D B. Power system static-state estimation, Part I: Exact model[J]. power apparatus and systems, ieee transactions on, 1970 (1): 120-125.
10. Schweppe F C. Power system static-state estimation, Part III: Implementation[J]. Power Apparatus and Systems, IEEE Transactions on, 1970 (1): 130-135.
11. Morrow K L, Heine E, Rogers K M, et al. Topology perturbation for detecting malicious data injection[C]//System Science (HICSS), 2012 45th Hawaii International Conference on. IEEE, 2012: 2104-2113.
12. Abur A, Exposito A G. Power system state estimation: theory and implementation[M]. CRC Press, 2004.
13. Gomez-Exposito A, Abur A, Rousseaux P, et al. On the use of PMUs in power system state estimation[C]//Proc. 17th Power Systems Computation Conference. 2011: 22-26.
14. Wood A J, Wollenberg B F. Power generation, operation, and control[M]. John Wiley & Sons, 2012.
15. Monticelli A. State estimation in electric power systems: a generalized approach[M]. Springer, 1999.
16. Hu X H. Interpretation of the latest developments in the international network warfare [J]. Information Security and Communications Privacy, 2009 (9): 7-9.
17. Chen J, Abur A. Placement of PMUs to enable bad data detection in state estimation[J]. Power Systems, IEEE Transactions on, 2006, 21(4): 1608-1615.

7 Acronyms

AGC: Automatic Generation Control
DC: Direct Current
ED: Economic Dispatch
EMS: Energy Management System
IED: Intelligent Electronic Devices

PMU: Phasor Measurement Unit
RTU: Remote Terminal Units
SCADA: Supervisory Control And Data Acquisition

Last Modified: December 1, 2014
This and other papers on current issues in network security are available online at http://www.cse.wustl.edu/~jain/cse571-14/index.html
Back to Raj Jain's Home Page