Contents lists available at ScienceDirect

The Electricity Journal

journal homepage: www.elsevier.com/locate/tej

False data attack models, impact analyses and defense strategies in the electricity grid

Xuan Liu, Zuyi Li*

Illinois Institute of Technology, Chicago, United States

ARTICLE INFO

Keywords:
False data attack
Attack model
Impact analysis
Defense strategy
Power system

ABSTRACT

The injection of false data is a type of cyber-attack that targets the data and measurements in power systems to disrupt their normal operation. This article presents a comprehensive review of such attacks against modern power systems from three perspectives: attack models, their operational impacts and defense strategies. Also discussed are future research directions in this field and existing technical challenges.

1. Introduction

The power grid is always a primary target of an attacker because of its importance to a nation’s economy and homeland security. An attacker can identify the weakness of a power grid and select the most vulnerable components as targets to attack (Arroyo and Galiana, 2005; Salmeron et al., 2009; Albert et al., 2000). The failures of these components lead to severe consequences to a power system, such as a large amount of loss of load (Motto et al., 2005) and cascading failures (US Canada Power System Outage Task Force, 2004; Carreras et al., 2002). In particular, when the system is heavily loaded, the outage of a single critical component may trigger a chain effect of component failures, finally leading to a blackout. From the view of an attacker, he or she can identify the weakness of the power grid and trigger the outages of these critical components by cyber-attacks. To maintain the security of the system, Supervisory Control and Data Acquisition (SCADA) systems are used to monitor and control power systems in real time by providing a bidirectional communications channel between remote infrastructures and the control center. However, the increasing integration of information technologies increases the vulnerability of SCADA systems to cyber-attacks. Further, more and more public Transmission Control Protocol/Internet Protocol (TCP/IP) is used in data transmission. These make SCADA systems even more vulnerable to cyber-attacks (Ten et al., 2008; Zhang et al., 2015).

The crisis of fossil fuels is a driver for the increasing penetration of renewable sources of energy such as wind and solar power. The intermittent and random natures of wind and solar power sources have significantly increased the uncertainty of power systems. Consequently, the operator’s situational awareness to the existence of bad data becomes weaker. In other words, the transmitted data should be regarded with greater fluctuation ranges due to a higher uncertainty of the system. This provides an attacker a good chance to alter the readings of sensors sent to the control center with a low probability of being detected. For instance, false attacks on the output power of a wind plant will not be easily detected if an attacker limits the attacking amount to within a reasonable range, since its output power itself fluctuates sharply with time.

The interconnection of power grids makes today’s power networks the largest man-made complex network, with thousands of buses and lines − more than 50,000 buses in the case of the East Interconnection (Tian et al., 2011). For such a large power network, it is very hard for the defender to protect all the sensors and secure all the transmitted data due to limited budget and resources. So far, a few phase measurement units (PMU) have been installed in a power grid. In addition, the wide spread of these sensors makes it harder to deploy protection devices. Thus, a large number of sensors are exposed to cyber-attacks.

This article presents a comprehensive review of false data injection attacks against modern power systems. The structure of this article is described in Table 1. Section 1 introduces the principle of undetectable false data injection attacks. Section 2 presents the attack models with complete and incomplete network information for transmission networks, distribution systems, and microgrids. Section 4 reviews the impacts of false data on the economic and secure operation of power systems. Section 5 summarizes different defense strategies against false data attacks. Section 6 discusses the future research directions in this field. Section 5 concludes the article.

* Corresponding author.
E-mail address: lizu@iit.edu (Z. Li).

http://dx.doi.org/10.1016/j.tej.2017.04.001

Table 1
Overview of the article.

Attack Models	Transmission Network	Yuan et al. (2011), Kim and Tong (2013), Liu and Li (2016a), Li et al. (2016), Chen and Abur (2006), Zhang et al. (2013), Xichen et al. (2013), Tate and Overbye (2008), Zhu and Giannakis (2012), Liu and Li (2016b), Hug and Giampapa (2012), Qin et al. (2012), Kim et al. (2014), Ozay et al. (2013), Dan and Sandberg (2010), Mohsenian and Leon-Garcia (2011), Ashfaqur-Rahman and Mohsenian-Rad (2012), Giani et al. (2013), Liu and Li (2014), Liu et al. (2015a), Liu and Li (2016c)
	Distribution Systems	Guo et al. (2014), Lim et al. (2010)
	Microgrid	Liu et al. (2016a), Beg et al. (2016), Li et al. (2017), Liu et al. (2015c)
Impact Analysis	Economy	Yuan et al. (2011), Liu et al. (2017), Xie et al. (2011), Choi and Xie (2014), Jia et al. (2014), Ye et al. (2016), Grochocki et al. (2012), Anwar et al. (2015), McLaughlin et al. (2009), McLaughlin et al. (2013), Salinas and Li (2016), McKenna et al. (2012), Sankar et al. (2013), Jokar et al. (2016)
	Security	Yuan et al. (2012), Liu and Li (2017), Liu et al. (2015b), Teixeira et al. (2012), Liang et al. (2016)
	Reliability	Zhang et al. (2016), Falahati et al. (2012), Falahati and Fu (2014)
Defense Strategies	Protecting critical measurements	Kosut et al. (2010), Kim and Poor (2011), Liu et al. (2016b), Esmalifalak et al. (2013), Mohsenian-Rad and Leon-Garcia (2011), Bi and Zhang (2011)
	Detecting false data	Bobba et al., (2010), Liu et al., (2014), Valenzuela et al. (2013), Weimer et al., (2012), Rawat and Bajracharya (2015), Zhao et al. (2015), Chakhchoukh and Ishii (2016), Manandhar et al. (2014), Li et al. (2015), Ashok et al. (2016), Esmalifalak et al. (2014), Mo et al. (2014)
	Increasing system's uncertainty	Rahman et al. (2014), Davis et al. (2012), Weerakkody and Sinopoli (2016)

2. Introduction of false data injection attacks

In real-world power systems, electric components, such as power plants and substations, are far away from the control center. Thus, a large number of sensors and a few number of PMUs are installed to obtain real-time measurements (e.g., bus injection powers, line flows, bus voltage) and send them to the control center for the next economic dispatch and security controls. Since measuring errors exist, it is essential for the operator to identify the corrupted data and get the best estimation of the real-time state of the power system.

The general principle of state estimation is to get the best estimate by the data consistency check method (e.g., least-square (Abur and Expósito, 2004)) according to the physical property of a system. The measurement vector $\boldsymbol{z}$ can be represented by the Jacobian function $\boldsymbol{h}(\boldsymbol{s})$, the state vector $\boldsymbol{s}$, and the vector of measurement errors $\boldsymbol{e}$. That is, $z = \boldsymbol{h}(s) + \boldsymbol{e}$. The goal of the state estimation is to determine the best $\boldsymbol{s}$ that minimizes the residual error.

In the direct current (DC) power flow model, $\boldsymbol{h}(\boldsymbol{s})$ is a constant matrix and does not depend on the state $\boldsymbol{s}$. Liu et al. (2009) for the first time considered the problem that if an attacker can construct such a false data injection attack that the overall residue of the system will not increase, the false data injection attack on measurements can bypass the residual test thus achieving a successful attack. For the alternating current (AC) case (Rahman and Mohsenian-Rad, 2013), the construction of the attack vector is more complicated as $\boldsymbol{h}(\boldsymbol{s})$ is not a constant matrix and depends on the state $\boldsymbol{s}$. In contrast to the DC case, the attacker needs to obtain the state $\boldsymbol{s}$ of the system for constructing a perfect attack vector that will not increase the residual.

3. Attack models

In this section, we will present the attack models with complete and incomplete network information for transmission networks, distribution systems, and microgrids.

3.1. Transmission system attacks

3.1.1. Attack models with complete network information

3.1.1.1. Load redistribution attacks. The general attack model in (Liu et al., 2009) shows that an attacker is able to inject false data into measurements without increasing the overall residual of the system if the full network information of a power grid is known to the attacker. However, it has some practical issues that limit its applications in real-world power systems. First, strong communication channels are usually built between power plants and a control center. Malicious modification of generations will be detected with a high probability. Second, the injected false power at a bus is assumed to be infinite. In practice, if the injected power at a bus is too large, such an attack can be easily detected with the assistance of load forecasting.

To provide a more practical attack model for studying the attack behaviors of an attacker, Yuan et al. (2011) introduced the load redistribution attack model by adding three practical constraints to the general attack model in (Liu et al., 2009): (1) The output power of a generator cannot be attacked due to the strong communications between the power plant and the control center; (2) Bus injection power measurement at a zero-injection bus in the power grid cannot be attacked since it is fixed to zero; (3) The attack amount at a load measurement should be limited within a certain range to reduce the situational awareness of an operator.

As the output powers of generators are attacked, the sum of attacked amounts at all load buses must be zero to ensure the power balance between consumption and demand. That is, such an attack is equivalent to redistributing loads at buses to achieve the goal of an attacker. Load redistribution attack is a special case of the general false data injection attack that can better capture the attack behaviors of an attacker.

3.1.1.2. Topology attacks. The topology of a power grid changes due to faults or forced outages (e.g., line switching) of transmission lines. To monitor the grid's topology, the status of transmission lines is sent to the control center in real time. If a line is in service, binary signal 1 will be sent. Otherwise, 0 will be sent to the control center to represent this line being out of service. During this data transmission process, an attacker has a chance to modify the status of a line sent to the control center because of the vulnerability of communication networks.

Kim and Tong (2013) demonstrated that the physical outage of a line can be simulated by launching the so-called state preserving attack without physically disconnecting this line, in which a pair of additional power increments is injected into the power measurements at the terminal buses of the attacked line. Notice that the attack only changes the power injections at the terminal buses of the attacked line, and the phase angles at all buses remain unchanged.

The drawback of the topology attack model in (Kim and Tong, 2013) is that the injected false power at a bus is assumed to be infinite. This is very impractical since an operator usually has some knowledge about the load distribution of a power grid and can predict future loads by load forecasting. Considering theses practical constraints, Liu and Li (2016a) proposed a local topology attack model that limits the injected power at a bus within a certain range. In particular, a heuristic algorithm is proposed to reduce the required network information for determining a feasible attack region.

Different from Refs. (Kim and Tong, 2013; Liu and Li, 2016a), Li et al., (2016) considered a novel topology attack model to mask the