Electrical Power and Energy Systems 104 (2019) 169–177

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

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

A two-layer game theoretical attack-defense model for a false data injection attack against power systems

Qi Wang[a,*], Wei Tai[a], Yi Tang[a], Ming Ni[b], Shi You[c]

[a] School of Electrical Engineering, Southeast University, Sipailou 2#, Nanjing, Jiangsu Province 210096, PR China
[b] NARI Group Corporation (State Grid Electric Power Research Institute), Chengxin 19#, Nanjing, Jiangsu Province 211000, PR China
[c] Department of Electrical Engineering, Technical University of Denmark, Elektrovej 325, Kgs. Lyngby, DK 2800, Denmark

ARTICLE INFO

Keywords:
False data injection attack
Game theory
Optimal load shedding
State estimation

ABSTRACT

With the widespread application of information and communication technology in power systems, cyber security has become critical for ensuring effective measurement, communication, calculation and execution. A successful false data injection attack (FDIA) can bypass traditional systems for identifying bad data and interfere with decision making in control centers, thus causing power system failures. In this paper, the measurements within the phasor measurement units (PMUs) are used as attack and defense objects, and load shedding resulting from line failure is utilized to quantify the attack consequences. To construct the optimal defense against an FDIA, this paper examines the characteristics and construction of FDIAs from the perspective of attackers, aiming to reveal the shortcomings of traditional bad data identification. From the perspective of those defending against an FDIA, a two-layer defense model is proposed that includes detection and protection. First, information from multiple sources is utilized to improve the detection of false data. Second, extra PMUs are added as a protection method to strengthen the measurement redundancy. A zero-sum static game algorithm is applied to optimize the deployment of defense resources. The effectiveness of the proposed strategy is tested using IEEE 14-bus, 57-bus and 118-bus systems, and the impact of information asymmetry is also discussed.

1. Introduction

With the development of advanced information and communication technology (ICT), traditional power systems have been upgraded into complex and multi-dimensional systems, i.e., cyber physical power systems (CPPSs) [1]. While these systems promote real-time analysis, decision support and efficient allocation of power resources, open communication networks and interface terminals also introduce potential cyber security risks [2,3]. Compared to relatively robust physical power systems, there are many undiscovered security vulnerabilities in the associated cyber systems. Cyber-attacks on power system operation and control can seriously impact the entire system, affecting safety, industrial production and people's livelihoods [4–6]. In recent years, a series of cyber-attacks against power systems have resulted in severe losses. A common example is the Blackenergy virus attack against the Ukraine power grid on December 23, 2015, which led to power outages lasting several hours for 700,000 households [7]. Moreover, it has been reported that there are over 2000 premeditated attacks on provincial power utilities in China every month [8]. As a novel attack mode that basic industrial facilities must contend with, both the attack mechanisms of cyber-attacks against power systems and defense strategies against such attacks require further study [9].

The targets of cyber-attacks against power systems can be classified into three categories based on their effects on security: availability, integrity and confidentiality of information [10].

1) Availability: communication interruption results in unavailable information;
2) Integrity: false data injection results in incorrect information;
3) Confidentiality: leakage and illegal usage of data.

A false data injection attack (FDIA) is a typical method of destroying information integrity. It is implemented by invading underlying distributed measurement terminals [11]. During the data transmission process of the power emergency control services, the rapid response demand causes a lack of encryption and detection ability in the smart measurement devices, which provides potential intrusion paths for the FDIA. The goal of an FDIA is to perform coordinated attacks against several buses and lines by falsifying measurements and manipulating state estimation data [12,13]. A well-designed FDIA can induce the

* Corresponding author.
E-mail addresses: wangqi@seu.edu.cn (Q. Wang), ni-ming@sgepri.sgcc.com.cn (M. Ni), sy@elektro.dtu.dk (S. You).

https://doi.org/10.1016/j.ijepes.2018.07.007
Received 23 April 2018; Received in revised form 31 May 2018; Accepted 5 July 2018

control center to misjudge the state of a power system and thus make poor decisions; this can severely threaten the economic efficiency, reliability and stability of the power system, even leading to cascading failures. Compared with control devices in unapproachable main stations, the measurement devices are mainly located in the user side with easier access. Therefore, from the perspective of attackers, FDIA is an effective means with enough practical feasibility.

In terms of attack process, researchers have investigated the process of injecting false data and tampering with measurement information under various conditions (e.g., different availability of security loopholes, bad data identification algorithms, power flow information and network topology in the power system) [14–16]. These studies aimed to explore the security vulnerabilities and vital regions of the system as critical parts of a defense. On this basis, the defense model is studied, including various procedures such as protection, detection, response, and recovery. In terms of protection, data encryption algorithms in the information layer are performed to reinforce the data security [17]. And to determine the critical measurements in the physical layer, some optimization algorithms such as fast greedy algorithm and bi-level mixed integer linear programming algorithm are taken to ascertain the critical region [18,19]. In terms of detection, intrusion detection mechanisms in the information layer, and bad data identification (e.g., the state estimation and machine learning based identification) in the physical layer are utilized to eliminate the FDIA impacts in the initial stage [20–22]. In terms of response and recovery, to mitigate negative attack effects, a corrective dispatch scheme is taken as countermeasures to achieve global flow optimum [23].

Most previous studies were based on inverting an actual FDIA procedure and attempting to determine attack mechanisms or defense strategies based on system vulnerabilities. The resulting solutions have generally been static, ignoring the interactions between the behaviors of attackers and defenders; the most vulnerable regions were examined as attack and defense objects.

In fact, if an attacker's possible actions are considered, the attack and defense objects selected through unilateral optimization strategies may no longer be the most vulnerable points. Furthermore, the resources that can be utilized by both sides are usually limited. To optimize attack and defense choices based on the actions of an attacker with limited resources, the original unilateral problem can be considered as a typical dynamic game process [24].

From the perspective of a joint game, most studies have focused on different attack-defense combinations and their impact on optimized resource allocation [25]. The goal of the game process is usually economic loss or stability reduction. Regarding economic loss, the power market price was used as an attack object in [26], and a Stackelberg game process was operated using a distributed learning algorithm to reflect the interactions between one defender and several attackers. Regarding stability reduction, in [27], a multistage stochastic game was used to examine an N-k attack against power lines. The state transition matrix was used to characterize the anticipatory actions of both players, and optimal load shedding was used to quantify the attack consequences. Similarly, in [28], attacks on power lines to cause load shedding were studied. A Markov model was utilized to simulate the dynamic interactions between two players. Both papers described above measured the attack and defense process based on the failure rate and repair rate of power lines. In [29], the economic index and the stability index were combined. The attackers attempted to infiltrate the power control networks to manipulate the transformers and power line breakers, while the defenders adopted generator re-dispatching to reduce power loss. Load shedding and generator tripping were used to quantify the economic benefits of attackers. The defender was only allowed to deploy an ex post remedy instead of premeditated defense.

Previous researchers focused on utilizing a dynamic game process to realize the optimal allocation of attack-defense resources. In general, they mathematically simplified the attack and defense mechanisms, resulting in inaccurate modeling of the attack process and consequences. In addition, these studies only examined how an attack on the control equipment would affect power system operations; they did not consider tampering.

The main purpose of this paper is to present an optimal decision-making strategy that considers an opponent's decisions during an FDIA against a power system. More specifically, this paper examines an FDIA aimed at phasor measurement units (PMUs). Based on PMUs with time scale calibration and high sample rate, the dynamic characteristics and whole appearance of the power system can be accurately determined. By harming observabilities of PMUs, attackers intend to cause unnecessary load shedding. The response by defenders involves deploying redundant PMU devices. Both attack and defense resources are limited; attackers must select optimal PMUs and defenders must deploy a limited number of redundant PMUs in the most effective defensive positions. A two-layer model is used to describe this attack and defense process. The upper layer includes the false data detection algorithm. It is improved by utilizing information from multiple sources (e.g., historical load data), which determines the threshold of the normal data. In the lower layer, the load shedding amount is used as a quantitative index and a zero-sum static game model is applied to balance the costs and effects of attack and defense. The model determines the dynamic equilibrium points of both players. To test the impact of the degree of information mastery on the attack-defense decisions, a scenario with information asymmetry is also considered.

The rest of the paper is organized as follows. In Section 2, the structure of the two-layer attack-defense model is introduced. In Sections 3 and 4, the upper layer process and the lower layer process are presented, respectively. Simulation results of the game process in IEEE 14-bus, 57-bus and 118-bus systems are given and discussed in Section 5. Section 6 gives the paper's conclusions.

2. Two-layer attack-defense model for FDIA against a power system

This study examines attack-defense strategies aimed at PMUs from the perspective of an intermediate observer. The attack follows the following steps: 1) formulate attack target and strategies; 2) falsify measurements by controlling meters, the communication network and the master station; 3) transfer the falsified measurements to the energy management system (EMS) and interfere with the estimation results; and 4) induce the control center to take emergency measures to trip critical buses and lines, resulting in load shedding. The detailed intrusion process is not discussed in this paper, which can refer to the related paper [30]. The attack resources are quantified as the number of PMUs that can be controlled, and the attack strategy is to force line overload by falsifying the measurements in the intruded PMUs.

The defense principle includes two steps: 1) protection-based defense and 2) detection-based defense. The former is used to protect critical sensors and measurements from intrusion using physical defenses (e.g., redundancy measurement configuration) before the FDIA, and the latter is used to identify modified data by mathematically analyzing measurements (e.g., identifying bad data and prediction based on historical patterns) after the FDIA. The redundant PMU deployment before the FDIA happens is utilized as the protection method, and the protection resources are quantified as the number of extra PMUs that can be deployed. The bad data identification afterwards is utilized as the detection method.

To apply game theory to these attack and defense mechanisms, a two-layer model of FDIA is established, as shown in Fig. 1. The upper model implements the detection-based defense, and the lower model implements the protection-based defense. In Fig. 1, the arrows marked with "Y" indicate an attack behavior that can be detected by the defense strategy, and "N" denotes the opposite. In the upper model, a real-time state database of the power system is generated using mixed measurement data. To detect possible false measurements, bad data identification procedures and an injection power detection module are