Electrical Power and Energy Systems 96 (2018) 368–379

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

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

Adequacy evaluation of electric power grids considering substation cyber vulnerabilities

Yingmeng Xiang[a], Lingfeng Wang[a,b,*], Yichi Zhang[c]

[a] *Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, Milwaukee, WI 53211, USA*
[b] *Dept. of Electrical Engineering and Computer Science, University of Toledo, Toledo, OH 43607, USA*
[c] *ATSEC Information Security Corporation, 9130 Jollyville Road #260, Austin, TX 78759, USA*

ARTICLE INFO

Keywords:
Cyber-physical systems
Power system adequacy evaluation
Human dynamics
Cybersecurity
Game theory

ABSTRACT

Modern cyber-physical smart power grids are becoming increasingly dependent on the associated cyber networks for performing various monitoring and control functions, which inevitably leads to increased cyber vulnerabilities. It is thus a pressing task to develop effective methods for comprehensively evaluating the overall adequacy of power systems considering the probable cyber vulnerabilities. This paper is focused on quantifying the impact of substation cyber vulnerabilities on power supply adequacy. The temporal occurrence pattern of cyber attacks is statistically analyzed based on the human dynamics theory. Also, the attack/defense interactions of intelligent attackers and defenders are modeled by static and Markov games in different attack scenarios. A novel power system adequacy evaluation framework is proposed by incorporating both physical failures and cybersecurity risks. Simulation studies are performed on a typical IEEE reliability test system, and the influences of critical factors related to cybersecurity are carefully investigated. These quantitative studies show that implementing effective cyber security measures and making informed decisions about the allocation of limited resources are beneficial to enhancing the overall adequacy of contemporary cyber-physical power systems.

1. Introduction

As one of the national critical infrastructures, power grids play an essential role in supporting the everyday life and economic development in the modern society. But unfortunately the contemporary power grid is vulnerable to various sabotages, cyber attacks, vandalism activities, terrorist attacks, and other emerging threats. The threat of cyber attacks against power system cyber networks is increasing dramatically due to the rapid development and integration of various cutting-edge smart grid technologies for performing advanced monitoring, control and protection functions. Specifically, there is a current trend to upgrade the power system substations based on IEC 61850 standards, where intelligent electronic devices (IEDs) and Ethernets are being deployed. Meanwhile, standardized Internet protocols are being deployed in the power system cyber structures, and supervisory control and data acquisition (SCADA) systems are being gradually connected to other networks, such as the business network or even the Internet, for improving operation flexibilities and reducing operation costs. All these changes could bring about possible cyber vulnerabilities, such as unsecured communication protocols and unauthorized remote access to the substation computers and IEDs. Also, weak cryptography and poorly-configured firewalls could be exploited by intelligent cyber intruders. In recent years, these cyber vulnerabilities related to electric power systems have received more and more attention [1].

Insecure cyber networks and increasing cyber intrusion activities could result in different levels of consequences on power systems ranging from disclosure of confidential information to disastrous large-scale blackouts. In history, multiple large blackouts have been caused primarily by incidents and failures related to the computing and communication infrastructure [2]. Recently it was reported that electric companies nowadays are in actuality under constant cyber attacks [3]. And it is very possible that these cyber attacks would occur more frequently as power system cyber networks are expected to become more interconnected with other networks in the future with the ongoing smart grid initiative.

There have been some recent studies on the cybersecurity of power systems. In [4], the impact of false data injection attack on power grid state estimation was modeled and a protection-based defensive scheme and a detection-based defensive strategy were proposed. A novel framework for modeling a variety of cyber-physical switching vulnerabilities was presented in [5]. Ref. [6] introduced a unified method to model the contingencies of cyber-physical systems based on various

[*] Corresponding author at: Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, Milwaukee, WI 53211, USA.
E-mail address: l.f.wang@ieee.org (L. Wang).

http://dx.doi.org/10.1016/j.ijepes.2017.10.004
Received 10 July 2017; Received in revised form 16 September 2017; Accepted 4 October 2017
0142-0615/ © 2017 Elsevier Ltd. All rights reserved.

malicious attack scenarios. The reliability of smart cyber-physical power grid was evaluated considering the cyber vulnerabilities in the SCADA network in [7]. In [8], the attack/defense interaction of the false data injection attack against the voltage control in smart grid was modeled by a stochastic game. In [9], the risk faced by the automatic generation control was quantified and a stochastic game is formulated to study the best response scheme of the attacker with limited resources. Despite these efforts, very limited research was conducted to evaluate the attack occurrence pattern and incorporate the cyber attacks into the power system adequacy assessment.

Power system adequacy evaluation aims to assess the power system's capability of supplying electric power to the customers without interruption while fulfilling the operational constraints. Currently in the field of power system adequacy assessment, the main focus is placed on investigating the influences of intermittent renewable energy resources [10] and the communication infrastructure failures [11–15]. In [11–13], the influence of the failure of phasor measurement units and their optimal placement on power system adequacy were studied. In [14–15], the reliability of wide-area measurement system was investigated and the methods to improve the reliability were explored. The accurate evaluation of power system adequacy requires taking into consideration all possible outages and uncertainties [16]. With the wider deployment of information technologies, it is possible that cyber attacks will happen more frequently in the future. Thus, it is highly necessary to incorporate the cyber attacks induced risk into power system adequacy evaluation.

In this study we aim to investigate the power system adequacy incorporating substation cybersecurity. Our research focus is associated with quantifying the impact of malicious cyber attacks on the overall power supply adequacy, while most of the aforementioned reliability assessment studies were focused on adequacy evaluation due to hardware failures. The adequacy analysis incorporating cyber attacks is very different from that based on random hardware failures, which is thus a particularly challenging task as explained in the following.

First, it is required to study the occurrence frequency of the cyber attack contingencies. The contingencies caused by hardware failures are considered as physical contingencies, and similarly the contingencies caused by malicious cyber attacks can be considered as cyber attack contingencies. The frequency of physical contingencies is mainly determined by the hardware's physical characteristics and the influence of the environment. But the frequency of cyber attack contingencies is mainly determined by the behaviors of malicious attackers, which involves a number of uncertainties. While sophisticated methods such as those based on Poisson distribution and state transition have been developed to study the frequency of physical contingencies, very little work has been conducted to statistically study the occurrence frequency of cyber attacks over a long time span [17]. This is primarily due to the unavailability of historical data coupled with privacy concerns. In this paper, human dynamics analysis is adopted to study the occurrence frequency of cyber attack contingencies as explained in Section 2.

Second, it is essential to study the consequence of each contingency. The influence of the physical contingencies is determined by the function and location of the hardware and the control strategy of the power system operator; simply speaking, it is unilaterally determined by the defender. However, the influence of the cyber attack contingencies is determined by the interaction between the attacker and the defender. It is an interactive process and more uncertainties are involved, such as the strategies, rationality and available resources of the attacker and the defender. In this study, game theory is applied to model the interaction between the attacker and the defender, and then to investigate the influence of each cyber attack contingency, which will be explained in Section 4.

The major contributions of this paper are summarized as follows:

(1) The cyber attack occurrence pattern in real scenarios is discovered, and it is analyzed with the human dynamics model.
(2) Based on the cyber attack occurrence pattern, the consecutive attack and individual attack are modeled by Markov game and static game, respectively, considering both the substation cybersecurity defense level and the repair time required to restore the substation.
(3) A holistic framework for assessing power system adequacy considering cyber attacks is proposed by integrating human dynamics and game theoretic modeling.
(4) A numerical study is developed to illustrate the proposed reliability evaluation framework, and the influence of multiple critical factors on system adequacy is studied.

The remainder of this paper is organized as follows. Section 2 statistically analyzes the cyber attack occurrence pattern and presents the human dynamics for interpreting the occurrence pattern. Section 3 introduces the cyber vulnerability of substations and discusses the consequence of cyber attacks considering the structure of the power system and the response of the system operator. Section 4 presents the game-theoretic study for modeling the substation attack-defense mechanisms under different cyber attack scenarios. Based on the attack occurrence pattern obtained in Section 2 and the consequence analysis obtained in Sections 3 and 4, a holistic power grid reliability evaluation framework is proposed in Section 5. Section 6 demonstrates the simulation outcomes and the analysis of critical parameters. Some practical issues are discussed in Section 7. Section 8 concludes the study and suggests potential future research directions.

2. Human dynamics analysis for cyber attacks

In order to analyze the influence of a contributing factor of power outages on the long-term statistic power system adequacy, it is essential to study its occurrence pattern. Conventionally, the Poisson distribution is adopted to model the failure of hardware components supported with the historical data. While it seems acceptable to assume that the cyber attack activities against power system could be simulated by Poisson distribution, many individual human activity temporal patterns were found to follow non-Poisson distributions, such as sending text messages, browsing webpages, and rating movies online [18,19]. Similar temporal characteristics have also been captured in many collective social behaviors, e.g., wars and terrorism attack events [20,21]. It is discovered that in these human activities the interevent intervals between two consecutive events are obviously not uniformly distributed. The time intervals are usually short, but there are also some non-negligible long intervals. By statistically analyzing the intervals τ, it is found that the probability $P(\tau)$ abides by the power law distribution:

$$P(\tau) \propto \tau^{-\alpha} \qquad (1)$$

where α is the exponent of the power law distribution, and it indicates the burstiness of the events. A larger value of the exponent indicates the burstiness of the event is more distributed.

A comparison between Poisson and power law distributions is illustrated in Fig. 1. Each vertical line in the figures represents a single event, and the mean values of the interval time are set to be the same. The sudden burst of a huge number of events in a short time period as well as inactivity within a long time period under power law distribution are more obvious than those in the Poisson distribution.

This study aims to develop appropriate methods instead of Poisson distribution to simulate the cyber attack occurrence pattern. However, until now very limited historical data about the cyber attacks targeting power grids are available to the public as the electric companies and utilities are concerned that the cyber attackers may take advantage of the data to increase their probability of launching successful cyber attacks. Also they have concerns on the loss of customers' confidence on their ability to provide high quality of service if these cyber incidents were released to the public. In this study, some real data [22] associated with the cybersecurity accidents are analyzed. These data record the detailed information on significant cyber attacks that occurred

Download English Version:

https://daneshyari.com/en/article/6859504

Download Persian Version:

https://daneshyari.com/article/6859504

Daneshyari.com