Electric Power Systems Research 151 (2017) 12–25

Contents lists available at ScienceDirect

Electric Power Systems Research

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

A game-theoretic study of load redistribution attack and defense in power systems

Yingmeng Xiang[a], Lingfeng Wang[a,b,*]

[a] Dept. 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

ARTICLE INFO

Article history:
Received 15 December 2016
Received in revised form 19 April 2017
Accepted 15 May 2017

Keywords:
Cybersecurity
Game theory
Budget allocation
False data injection attack
Bilevel optimization

ABSTRACT

The wide deployment of advanced computer technologies in power systems monitoring and control will inevitably make the power grid more vulnerable to various cyber attacks. Load redistribution (LR) attack is regarded as a typical and viable cyber attack against power grids, which may mislead the power re-dispatch and cause unnecessary load loss. It is critical to develop methods for optimal allocation of limited defensive resources to safeguard the power grid, especially those considering the probabilistic behaviors of the attackers. To prevent the LR attacks, the optimal budget allocation and the game-theoretic attack and defense interaction are studied in this paper. Specifically, the attack and defense interactions are incorporated in the bilevel modeling of LR attacks. A few important substations are selected based on their criticality as cyber protection targets. For defending the critical substations, an optimal budget allocation strategy is developed to minimize the expected load loss subjected to the attacker's capability. Further, cybersecurity reinforcement strategies are studied using game-theory based approaches for different attack scenarios. The proposed methods are tested in different scenarios based on an IEEE test system, and the simulation results validate that the proposed methods are effective. This study offers new insight into preventing and mitigating the LR attack effectively.

© 2017 Elsevier B.V. All rights reserved.

1. Introduction

In response to worldwide initiatives to protect the environment and promote resource reservation, the next-generation power grid is being developed around the world. A great difference between the smart grid and the traditional grid lies in the broader adoption of various advanced intelligent devices and the associated cyber information and control technologies. Typical novel application examples are IEC 61850 based substations, smart meters, phasor measurement units, etc. [1]. Also, electric vehicles are integrated into the power systems [2]. Advanced demand response [3] and congestion management [4] strategies are being proposed and implemented. All these applications gradually transform the power grid to a cyber-physical smart grid, and they bring greater operation flexibility to the power grid while making the power grid reliability increasingly dependent on the associated cyber network. However, with the expansion of the cyber layer of the power grid, cyber vulnerabilities in the cyber components are inevitably incurred and the power grid is susceptible to various kinds of cyber attacks. For example, the attackers could intrude into the wide area communication network, launch the man-in-the-middle attack to intercept and then manipulate the commands sent to the breaker. And the lines or generators could be tripped and the power system operation is disrupted. Also, attackers can crack the password or exploit the vulnerabilities in the supervisory control and data acquisition (SCADA) network to manipulate the measurements transmitted to a control center. Alternatively, attackers can initiate denial-of-service attack to block or delay the communication between the control center and the substations. This might cause loss of system synchronism or unavailability of critical field devices. These cyber attacks could possibly bring disastrous impacts to the power grid, and in reality cyber incidents/attacks in the energy sector have happened worldwide [5]. The cybersecurity issues of the power system have received great attention recently [6,7].

As an essential function in the energy management system, state estimation helps the power grid operator gain an accurate understanding of the real-time power grid state and serves as the foundation for power system operations. If the state estimation outcome is compromised, the power system operator could be misled and uninformed decisions may be made. Recently it was found in Ref. [8] that by deliberately changing the measurements,

[*] Corresponding author at: Dept. 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.epsr.2017.05.020
0378-7796/© 2017 Elsevier B.V. All rights reserved.

Nomenclatures

Indices

i	Index for the loads
j	Index for the lines
h and h'	Index for the buses
k	Index for the generators

Sets

B_D	Set of loads
B_F	Set of lines
B_G	Set of generators
$\emptyset_c$	Set of critical substations

Parameters

H	The Jacobian matrix of the power grid
SF	The shift factor matrix
BL	The bus-load incidence matrix
BG	The bus-generator incidence matrix
E	A unity matrix
P_D	The load demand vector
τ	The percentage indicating the limitation on the attack on the load demand measurement
n_b	The total number of lines in the power system
$P_{F,j}^{\max}$	The transmission capacity of the line j
$P_{G,k}^{\min}/P_{G,k}^{\max}$	The minimum/maximum active power output of generator k
r_{total}	The total defensive budget
Δr	The minimal allocable unit

Variables

ΔZ	The attack on the measurement
ΔX	A non-zero vector
ΔP_F	The attack on line power flow measurements
ΔP_D	The attack on load measurements
$w_{h,h'}$	The normalized weight of the line between bus h and h'
$B_{h,h'}$	The betweenness of the line between bus h and h'
$\theta_{h,h'}$	The number of times the shortest paths for arbitrary two nodes traversing the line between h and h'
E_h	The entropic degree E_h of bus h
N_c	Number of critical substations selected for protection
N_p	The total number of possible targets
N_m	The maximum number of critical substations the attackers could attack subject to their capacity
N_t	The number of potential targets when N_m of the N_c critical substations are selected
N_s	The size of the game states with N_c critical substations
r	Vector of the budget allocation
$\xi_c(r_c)$	The substation protection function for the c-th critical substation
m	A target of the attack
φ	A successful attack scenario characterized by the set of successfully compromised critical substations
f_φ	The gain of the attackers for a successful attack scenario φ
$P_{C,i}$	The load curtailment on load i
$P_{F,j}$	The power flow on line j
g	Number of critical substations in target m
$U_m(r)$	Expected load loss for target m with budget allocation vector r
$q(m)$	Possibility that the attackers select the target m
$L(r)$	The maximal loss for budget allocation vector r
$n\_\max$	The fastest descent substation for all the first-order partial derivatives of $L(r)$
$\vartheta, \mu, \underline{\alpha}_j, \bar{\alpha}_j, \underline{\beta}_k, \bar{\beta}_k, \underline{\gamma}_i, \bar{\gamma}_i$	Lagrange multipliers
S	Set of the game states
ξ^s	The probability describing the performance of the security administrators' actions.
ξ^{and}	Probability for a secure substation to become compromised when it is attacked but not reinforced in a time step
ξ^{ad}	Probability for a secure substation to become compromised when it is attacked and also reinforced by the defenders in a time step
ξ^{ar}	Probability for a compromised substation to become secure when it is being restored by the defenders while it is also attacked in a time step
ξ^{nar}	Probability for a compromised substation to become secure when it is being restored by the defenders while it is not attacked in a time step
$T(s, a_a, a_d, s')$	The transition probability from state s to state s' with actions a_a, a_d
pa	The probability of selecting a pure strategy
γ	The discount factor in Markov game
N_a/N_d	The number of critical substations the attacker/defender chooses to attack/strengthen in a time step
a_a/a_d	The attackers'/defenders' action strategy
S_{N_a}/S_{N_d}	The set of all the possible combinations of selecting $N_{\rm a/}N_{\rm d}$ target substations out of the total N_c critical substations
π_a/π_d	The attackers'/defenders' mixed strategy
π_A/π_D	The attackers'/defenders' mixed strategy space
G_a/G_d	The expected reward for the attackers/defenders
Q_a/Q_d	The expected cumulative reward for the attackers/defenders
V_a/V_d	The expected optimal long-term reward for the attackers/defenders

attackers could pass the bad data detection and manipulate the outcome of the state estimation purposely. Further, in Refs. [9] and [10], a practical false data injection attack termed load redistribution attack was proposed, and two mathematical models considering the immediate consequence and delayed consequence were studied. In these two papers, the interaction between the attackers and the defenders was modeled by bilevel optimization, which is widely used in the power system security analysis and energy management [11].

There have been multiple studies about the defense schemes against the cyber attacks. In Refs. [12] and [13], it was proven that attackers only need to know part of the power grid structure information in order to compromise the outcome of the state estimation. In Ref. [14], a graphical approach was proposed to secure carefully selected measurements to defend the power grid against false data injection attacks using the AC power system model. In Ref. [15], protection-based and detection-based defense methods were investigated to identify the important measurements for making the power grid resilient to the false date injection attack. In Ref. [16], the attack and defense of bad data injection in electric power market was studied with a game-theoretic approach. The attack and defense interaction between the attackers and defenders was analyzed by Markov-game for the voltage control in Ref. [17] and automatic generation control in Ref. [18]. The cyber-physical

Download English Version:

https://daneshyari.com/en/article/5000998

Download Persian Version:

https://daneshyari.com/article/5000998

Daneshyari.com