Electrical Power and Energy Systems 101 (2018) 127–138

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

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

Observer-based cyber attack detection and isolation in smart grids

Xiaoyuan Luo[a,*], Qian Yao[a], Xinyu Wang[a], Xinping Guan[b]

[a] School of Electrical Engineering, Yanshan University, Qinhuangdao 066004, China
[b] School of Electronic and Electric Engineering, Shanghai Jiaotong University, Shanghai 200240, China

ARTICLE INFO

Keywords:
Smart grid system
Cyber attack
Attack detection and isolation
Graph theory
Modified observer

ABSTRACT

In this paper, we investigate the cyber security problem for large scale smart grid systems under false data injection attack. An observer-based algorithm is proposed to detect and isolate the cyber attack by using real-time synchrophasor measurements. Combining the smart grid system with graph theory, the system is divided into several different coupled areas via sparsity of the connection topology. According to the partition, the system is decomposed equivalently into several areas. Then, the output of the smart grid system can be gotten through wide area measurement system based on PMUs, and the asymmetric weighted Laplacian can be obtained by running a nonlinear least-square estimation algorithm. By designing a modified observer, the residual is computed, and the adaptive residual threshold, used to detect and isolate the attack in the areas of the system, is also shown with considering the system model uncertainties. Then, an iterative algorithm detecting and isolating the cyber attack is proposed based on the calculated residual threshold. Finally, some simulations are provided to illustrate the effectiveness of the proposed algorithm.

1. Introduction

The smart grid system [1] is the focus of the global power industry, leading the direction of future development of the electric-power industry, and it is widely used in various regions of the world. The smart grid system is one of the largest and most complex mechanical engineering. However, due to the complexity and openness characteristics of the system, the security features of smart grid system [2,3] are particularly worthy of our attention. On the one hand, many structural units of the system exist serious uncertainty and unreliability, which are prone to cause infrastructures' hardware and software failure. On the other hand, due to the open nature of the communication network, the system may be subject to malicious attacks [4–6], which can cause a serious impacts on the stability and control performance of smart grid system. In order to enhance the security of smart grid system against attacks, the academic and industry researchers have paid a great attention, and many significant research works have been made.

In this context, [7] studied the required minimum actuation energy for the adversary to attack the goal using the relativity of the inverse of controllability Gramian, and analyzed the vulnerability of linear network synchronization processes. [8] provided constructive algebraic conditions to cast undetectable and unidentifiable attacks, and described graph-theoretic conditions for the existence of undetectable and unidentifiable attacks. The centralized approach to detect all the possible attacks based on the system observability was proposed in [9]. But as a matter of fact, the smart grid system is a kind of large-scale network system, the centralized approach often requires all the information of the generators, which has a lot of difficulties in the actual situation. A distributed method was studied in [10], in which it divided the system into multiple modules, and then the output of the system was obtained by using the iterative method. [11] developed the dynamic state estimation methods based on cubature Kalman filter under cyber attacks. [12] detected the attack in the system according to a novel quasi-decentralized functional observer. [13] used an H_∞ approach to guarantee distributed input attack detection by neighbors' state estimation to track the attack input. However, the change of system dynamic model in real time is not considered, it is necessary to obtain the real-time system matrix, to date the nonlinear least square method which is the most widely used method. Under this background, wide-area measurement systems consisting of hundreds of new phasor measurement units (PMUs) have been put forward to measure the output of the system in real time. In the current state-of-the-art, most of the researches about PMU data were mainly used for off-line analysis such as monitoring of robust state estimation, identification of dynamic events taking place in the system and the generator pairs going out of synchronism [14–16]. However, a very limited amount of researches have evaluated beyond offline analysis, and the PMU measurements are necessary to be used for online detection for large scale smart grid systems. Meanwhile, attack detection for the multiple-input multiple-output large scale smart grid systems is considered in the presence of

[*] Corresponding author.
E-mail addresses: xyluo@ysu.edu.cn (X. Luo), 523923767@qq.com (Q. Yao), 1984604729@qq.com (X. Wang), xpguan@sjtu.edu.cn (X. Guan).

https://doi.org/10.1016/j.ijepes.2018.02.039
Received 1 June 2017; Received in revised form 5 January 2018; Accepted 22 February 2018
0142-0615/ © 2018 Elsevier Ltd. All rights reserved.

unknown attack inputs, then the attacks are difficult to be detected and isolated due to the system coupling structure. Therefore the coupling relationship in this paper is further studied and decoupling measures are proposed.

In the paper, we propose a state observer-based algorithm for the large scale smart grid systems to detect and isolate the unknown attack. Firstly we consider the linear continuous time descriptor model of a smart grid system [17,18]. Taking the large scale smart grid system into account, it may be intractable to harvest all data and information practically, our goal is to find a partitioning in which the worst node has more internal than external connection and the worst area has more internal than external connections, that is, the system can be divided into some areas via sparsity of connection topology, therefore, the connections within a area are dense while the connections between areas are sparse. Assuming the attack [19] enters through the electromechanical swing dynamics of the synchronous generators in the smart grid system, we consider the uncertainties of the system model, then it can be determined by running a nonlinear least-square (NLS) algorithm based on the dynamic data acquisited from PMUs. Furthermore, in order to detect and isolate the attacks in smart grid system we propose a new full order state observer for attack detection. Consider the multiple-input multiple-output large scale smart grid system, then we design suitable observation matrix to achieve the corresponding relation between the residual of the state observer and the input of the smart grid [20,21]. The residual is generated by using the prior knowledge and measurement to obtain the function containing the cyber attack information, and then the residual is computed according to the adaptive threshold [22,23] for cyber attack detection and isolation.

The rest of the paper is organized as follows. Section 2 introduces some basic concepts of graph theory. Section 3 formulates the regional division problem of the large scale smart grid systems. Then a new full order attack detection observer is designed and a corresponding algorithm for cyber attack detection and location is also proposed in Section 4. Some simulation results are provided in Section 5 to demonstrate the effectiveness of the proposed algorithm. Section 6 concludes this paper.

2. Preliminaries

2.1. Graph theory

We consider a graph $G=(\nu,\varepsilon)$ consisting of the vertices (or nodes) set $\nu=\{1,...,n\}$ and edges set $\varepsilon\in\nu\times\nu$. If there is an edge $kl\in\varepsilon$, the nodes $k,l\in\nu$ are adjacent, which we can write $k\sim l$. The set of the nodes adjacent to $l\in\nu$ also can be called the neighborhood of l as $N_l=\{k\in\nu|k\sim l\}$. The graph G is assumed to be undirected in this paper. We assume that every edge $kl\in\varepsilon$ has a real valued weight $a_{kl}=a_{lk}>0$, and every node $k\in\nu$ has a real valued weight $m_k>0$. In a smart grid system model, the edge weight is proportional to tie-line admittance and the node weight corresponds to the generator inertia constant. Then the symmetric positive semidefinite graph Laplacian matrix L_G of Graph G can be defined as

$$[L_G]_{kl}=\begin{cases}-a_{kl} & \text{if } k\sim l\\ \sum_{i\in N_k} a_{ki} & \text{if } k=l\\ 0 & \text{otherwise}\end{cases} \tag{1}$$

Therefore we can also define the asymmetric positive semidefinite graph Laplacian matrix $L_m\triangleq M^{-1}L_G$, where $M=diag\,[m_1,...,m_n]\in\mathbb{R}^{n\times n}$ is the generator inertia constant matrix.

2.2. Cartesian product graph

Definition 1. (Cartesian product graph [24]): Assume a case where, there are any two graphs $G_1=(\nu_1,\varepsilon_1)$ and $G_2=(\nu_2,\varepsilon_2)$, hence the Cartesian product graph G has the vertex set $\nu=\nu_1\times\nu_2$ and vertices $(i_1,i_2),(j_1,j_2)\in\nu$ which are adjacent if and only if either $i_1=j_1$ and $i_2j_2\in\varepsilon_2$ or $i_2=j_2$ and $i_1j_1\in\varepsilon_1$.

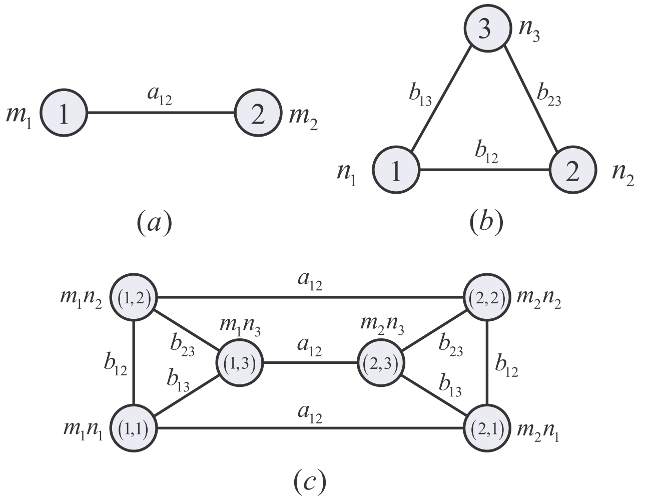

Fig. 1. Node- and edge- weighted graph product: (a) A 2-node graph, (b) A 3-node graph, (c) Result of the product of graph (a) and (b).

An example of the Cartesian product graph is shown in Fig. 1, where Fig. 1(c) denotes the result of the node- and edge- weighted graph product of Fig. 1(a) and (b).

Remark 1. For the remainder of this section, an arbitrarily-large n-area complete graph may also be constructed using Definition 1 and then the division of regional in a way preserves the complete property.

3. Problem formulation

In this section, we will depict the model of smart grid system [25] and formulate the regional division problem.

3.1. Smart grid system model

We consider an n-bus smart grid system with n_g generators buses and $n-n_g$ load buses. Let $b_i,i\in\{n_1,...,n_g\}$, denote the generator buses, and $b_k,k\in\{n_{g+1},...,n_n\}$, denote the load buses. Denote inertia constant m_i, damping constant d_i, rotor angle δ_i, frequency ω_i, mechanical power input P_{mi} and its electrical power output P_{ei} for generator $g_i,i\in\{n_1,...,n_g\}$. Then the rotor dynamics swing equation of generator g_i can be given as follows [8]

$$m_i\ddot{\delta}_i=P_{mi}-P_{ei}-d_i\dot{\delta}_i,quadi\in\{n_1,...,n_g\}. \tag{2}$$

where the electrical power output P_{ei} injected into the generator terminal bus b_i is given by

$$P_{ei}=\sum_{j\in N_i} V_iV_jG_{ij}\cos(\delta_i-\delta_j)+V_iE_jB_{ij}\sin(\delta_i-\delta_j) \tag{3}$$

where N_i means neighbor node set of node i,V_i and E_j are the voltage modulus of bus b_i and generator g_j,G_{ij} and B_{ij} are the mutual conductance and susceptance, respectively.

Next we make the following assumptions for the linearization methods of the smart grid system.

Assumption 1. The power network system is lossless.

Assumption 2. The relative rotor angle differences are sufficiently small.

Remark 2. Assumption 1 is due to the ultrahigh voltage power transmission, then we can deal with the conductances as zero, since the objective is to isolate the unknown input such as cyber attack in a reduced order model consisting of long tie-lines. And the nonlinear

Download English Version:

https://daneshyari.com/en/article/6859232

Download Persian Version:

https://daneshyari.com/article/6859232

Daneshyari.com