Information Systems 53 (2015) 201–212

Contents lists available at ScienceDirect

Information Systems

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

Identification of vulnerable node clusters against false data injection attack in an AMI based Smart Grid

Adnan Anwar [a,*], Abdun Naser Mahmood [a], Zahir Tari [b]

[a] School of Engineering and Information Technology (SEIT), The University of New South Wales Australia, Canberra, ACT 2610, Australia
[b] School of Computer Science and IT, RMIT University, Melbourne, VIC 3001, Australia

ARTICLE INFO

Article history:
Received 1 June 2014
Received in revised form
10 November 2014
Accepted 1 December 2014
Available online 8 December 2014

Keywords:
False data injection attack
Radial distribution networks
MatPower
Vulnerable nodes
CFPSO clustering

ABSTRACT

In today's Smart Grid, the power Distribution System Operator (DSO) uses real-time measurement data from the Advanced Metering Infrastructure (AMI) for efficient, accurate and advanced monitoring and control. Smart Grids are vulnerable to sophisticated data integrity attacks like the False Data Injection (FDI) attack on the AMI sensors that produce misleading operational decision of the power system (Liu et al., 2011 [1]). Presently, there is a lack of research in the area of power system analysis that relates the FDI attacks with system stability that is important for both analysis of the effect of cyber-attack and for taking preventive measures of protection.

In this paper, we study the physical characteristics of the power system, and draw a relationship between the system stability indices and the FDI attacks. We identify the level of vulnerabilities of each AMI node in terms of different degrees of FDI attacks. In order to obtain the interdependent relationship of different nodes, we implement an improved Constriction Factor Particle Swarm Optimization (CF-PSO) based hybrid clustering technique to group the nodes into the most, the moderate and the least vulnerable clusters. With extensive experiments and analysis using two benchmark test systems, we show that the nodes in the most vulnerable cluster exhibit higher likelihood of destabilizing system operation compared to other nodes. Complementing research is the construction of FDI attacks and their countermeasures, this paper focuses on the understanding of characteristics and practical effect of FDI attacks on the operation of the Smart Grid by analysing the interdependent nature of its physical properties.

1. Introduction

In recent years, several cyber related attacks, including the sophisticated Stuxnet worm attack [2], have highlighted the importance of security research in the area of Smart Grid infrastructure. It has been shown that a cyber-attack on the Smart Grid can cause devastating impact on our daily life resulting in cascading failures of critical Smart Grid infrastructure and disruption in economy. Sophisticated new attacks have emerged, targeting the increased use of intelligent devices (such as Smart Meters) in today's Advanced Metering Infrastructure (AMI) of the Smart Grid. There are different of kinds of attacks on the Smart Grid, including attacks on data availability, data confidentiality and data integrity. An example of data integrity attack is where a vital component of Smart Grid operational module can be affected by injecting false data into the AMI. Recently, these types of attacks, typically known as False Data Injection (FDI) attacks [3], have drawn significant attention as they can bypass the current security measures and exploit the system operations such as the state estimation process.

* Corresponding author. Tel.: +61 451001357.
E-mail address: Adnan.Anwar@adfa.edu.au (A. Anwar).

http://dx.doi.org/10.1016/j.is.2014.12.001
0306-4379/

State estimator, which is widely used at the utility control centres to calculate the system status during the power system operation, can also be used to filter out the measurement errors and noises [4]. Generally, 'state estimator' can be defined as a computer program which calculates the system states based on the measured data (at different nodes of the Smart Grid) and the equivalent modelled data (based on Kirchhoff's current and voltage laws of physical energy grid). In addition, the Bad Data Detection (BDD) module of the state estimator suppresses any bad data (if exists) based on the residual analysis. Generally, the traditional SE module works based on the principle of Weighted Least Squared (WLS) error minimization method where attack or noise is detected based on the residual analysis [4]. Liu et al. show that the Smart Grid state estimators are now highly vulnerable to the cyber attacks [3]. In the first work of these types of FDI attacks, Liu et al. show that the attack cannot be detected by the residual analysis if certain strategies are followed. Till then, significant research works have been carried out from both attacker's and defender's point of view, discussed below.

Authors in [1] develop some heuristic approaches to exploit the DC state estimation considering both random attacks and targeted attacks. Ozay et al. further extend the work by considering distributed models to generate and detect sparse attack in the state estimation process of the Smart Grid [5]. Different threats of Advance Metering Infrastructure (AMI) are also explored in the literature [6]. Defense strategies of the state estimation module and AMI devices are also well studied [7–10]. For example, a defense strategy based on graphical models to protect Smart Grid against FDI attack is proposed in [7]. In that work, authors consider a dc approximate model of the Smart Grid. Another dc approximate model based protection and detection mechanism is proposed by Yang et al. [8]. Typically, Smart Grid has non-linear power flow characteristics and an ac model of power flow equations can ensure more accurate results. Analysing and comparing with ac model, Hug et al. in [9] show that FDI attacks based on a dc model are more prone to introduce errors in the measurement devices resulting higher probability of detection through BDD technique. To protect AMI, an intrusion Detection framework based on consumption pattern of the end-users is proposed in [10]. Although significant number of research works have been conducted on simulating the FDI attacks [1,5,6] and determining the countermeasures [7–10], there are significant scopes to understand the security vulnerabilities of Smart Grid against FDI based cyber attacks by analysing the physical behaviours of the Smart Grid. Moreover, most of the existing FDI attack simulation and defense strategies are based on the transmission system [3,1,5,7–9] and there is a lack of research works considering power distribution systems. Traditionally, power distribution system has district characteristics from transmission system, e.g., high Resistance to Reactance Ratio, radial network, etc. Therefore, it is important to conduct the vulnerability analysis considering benchmark power distribution systems.

In this work, we have studied the interdependent nature of nodes in a power grid and identified the vulnerable nodes that are most sensitive to False Data Injection (FDI) attacks. We have found that if the attacker specifically targets these highly vulnerable nodes, then the attack will cause much larger impact destabilizing the operation of the power grid than any random selection of nodes. For example, if the same attack vector is introduced as an FDI attack at different measurement nodes, the power system operational states (e.g., Voltage Magnitude and Angle) will vary differently based on the physical properties of the individual nodes. The most vulnerable node identified in our analysis has the largest changes of the operational states and the opposite characteristics are observed for the least vulnerable node. This research is important from both attacker's and system operator's (defender) point of view. Based on the understanding of the node characteristics of the physical Smart Grid, the attacker can decide which node to attack to ensure significant changes of the operational states. On the other hand, the system operator (act as a defender) can emphasis on the real-time monitoring of the vulnerable nodes and introduce proper security measures (e.g., real-time Intrusion Prevention and Detection systems) on those locations. Besides, a distribution system state estimation in a Smart Grid, which has different characteristics from the widely used transmission system state estimation, makes use of AMI measurements instead of pseudo-measurements to enhance the state estimation performance [11]. These AMI measurements are deployed at the end-user nodes. The output of the Smart Grid state estimation will be corrupted if an attacker injects False Data in those AMI measurement devices. In this work, we also conduct vulnerability analysis at different AMI measurement nodes with different degrees of FDI attacks.

Specifically, the contributions of this paper are as follows:

(1) In contrast to existing work on FDI attacks that lack comprehensive power system analysis of the effect of the FDI, in this paper we provide a theoretical study of the relationship between FDI attack vectors and their effect on nodal and system stability (Section 2.3). We show that the Voltage Stability Index (VSI) [12], which is widely used by Power System engineers to determine the system stability [13,14], can also be used to understand the likelihood of system stability under different degrees of FDI based cyber attacks. To the best of our knowledge, this paper, for the first time, considers the voltage stability based indices to understand the cyber-physical vulnerabilities under any information integrity attack (e.g., FDI attacks) of a smart power distribution system.
(2) In order to properly identify nodes with similar levels of vulnerabilities in a complex system, we propose and implement a hybrid clustering algorithm based on the traditional well studied k-means algorithm and the Constriction Factor Particle Swarm Optimization (CF-PSO) to enhance the clustering performance. Experiments performed using test data from UCI repository of machine learning databases show that the CF-PSO based improved clustering outperforms the traditional k-means algorithm and the CF-PSO based clustering. This improved clustering algorithm is then employed to identify nodes that behave similarly based on their physical properties in response to an FDI attack.