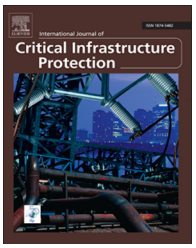
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Phasor measurement unit selection for unobservable electric power data integrity attack detection

Annarita Giani[a,*], *Russell Bent*[b], *Feng Pan*[b]

[a]DSA-4, CNLS, Los Alamos National Laboratory, P.O. Box 1663, Los Alamos, NM 87545, USA
[b]DSA-4, Los Alamos National Laboratory, P.O. Box 1663, Los Alamos, NM 87545, USA

ARTICLE INFO

Article history:
Received 12 January 2014
Accepted 25 March 2014
Available online 25 June 2014

Keywords:
Smart grid
Synchrophasors
Phasor measurement units
Cyber security
Unobservable data integrity attacks
Integer programming

ABSTRACT

Electric power system operators make critical decisions based on remote measurements. If the measurements are compromised, the decisions made on the basis of the bad measurements could lead to critical consequences. Of particular concern are unobservable attacks where compromised measurements are not flagged as erroneous by bad data detection algorithms. Secure measurement devices, such as phasor measurement units (PMUs), can help to recognize these attacks. This paper presents an algorithm based on integer programming for the optimal placement of PMUs to detect unobservable electric power SCADA data integrity attacks. The algorithm can also be used to identify minimal sets of existing PMUs whose data is needed to detect unobservable bad data attacks. Practical examples drawn from the power engineering literature are used to demonstrate the efficiency of the algorithm.

1. Introduction

Modern societies and economies are increasingly dependent on services such as electric power, natural gas and water provided by infrastructure systems. These systems are highly complex and are governed by highly non-linear relationships. The complexity makes the systems very difficult to control and operate. Despite the complexity, considerable progress has been made in recent years to improve the control and operation of infrastructure systems. The smart grid initiatives are an example of such an advance [7,8]. Smart grid control processes are highly dependent on accurate system state data that is remotely measured and transmitted to control systems via advanced supervisory control and data acquisition (SCADA) systems. The transmission of data represents a point of vulnerability of the smart grid to cyber attacks.

This paper focuses on data integrity attacks on SCADA systems used for electric power distribution. Currently, SCADA devices in power systems measure system states such as power injections at substations (buses), power flows at lines and transformers, and voltage values (magnitudes). Historically, such data is measured and transmitted with the expectation that there is noise and error in the measurements and that it does not provide enough information (e.g., voltage phase angles) to completely characterize the system state. As a result, the power engineering community has developed sophisticated techniques to estimate the state of unobserved portions of the power grid and to filter bad data [17]. These techniques are robust to random failures and expected measurement errors in power systems. However, there is increasing concern that it is possible to introduce errors in the data in a coordinated manner that is undetectable by bad data filters [14]. When an error is

*Corresponding author.
E-mail address: annarita@lanl.gov (A. Giani).

http://dx.doi.org/10.1016/j.ijcip.2014.06.001
1874-5482/

introduced by a malicious source (e.g., cyber attacker), the error is referred to as a "data integrity attack." When attack data is provably able to bypass bad data filters, the corresponding attack is referred to as an "unobservable" data integrity attack [14]. In general, an unobservable attack requires the compromise of a large number of sensors and recent work has focused on developing general methods for identifying the worst case scenarios based on the numbers of sensors that are compromised [5,9,11,14]. While these methods are important for assessing system vulnerability, the computational requirements are high and the problems tend to be very difficult to solve.

Some unobservable data integrity attacks only require a small number of compromised sensors. It can be argued that such attacks are more realistic because an attacker has limited resources (e.g., time and information) to plan an attack. These types of attacks are referred to as k-sparse attacks, where k is the number of sensors that are compromised [9,14]. Recent research [9] has shown that identifying all possible 3- 4- and 5-sparse attacks requires polynomial time, which eliminates the computational challenges associated with more general models. More importantly, perhaps, the research [9] has identified the types of redundant measurements that are required to make unobservable k-sparse attacks detectable. One important measurement for detecting k-sparse attacks is the voltage phase angle (other measurements, such as frequency and line flows, can also be used for this purpose).

Voltage phase angles are typically estimated from other measurements. Since phasor measurement units (PMUs) directly provide these measurements [18], they are candidate devices for detecting unobservable attacks. This paper develops optimization models for optimally placing PMUs to cover undetectable attacks. Alternatively, in the case where PMU deployment is ubiquitous, optimization models can be used to identify the smallest set of PMUs for detecting attacks.

The PMU placement problem is generally an NP-complete problem. As discussed in [9], the specific placement problem considered in this paper is not different. However, limited research has focused on optimizing the placement of PMUs to combat k-sparse attacks. While it is possible to optimize the placement of PMUs using a polynomial time algorithm that is guaranteed to find a sufficient number of PMUs [9], it does not yield the optimal solution. This paper describes a model that is guaranteed to find the optimal solution. In the worst case, the algorithm requires exponential time, but it has proved to be efficient when tested on a wide range of practical problems.

Several researchers have focused on similar PMU placement problems. Some of the research seeks to determine the optimal placement of PMUs to improve system observability [1,2,15,20,24]. Other research seeks to maximize the amount of mutual information between PMU measurements and power system states [12]. Yet other research [13] considers multi-objective criteria such as observability, cost, importance and security or poses the PMU placement problem in terms of improving state estimation [3,4,12]. Interested readers are referred to [26] for a comprehensive coverage of PMU allocation problems and their solutions.

This paper has three main contributions with regard to the detection of electric power data integrity attacks. The first contribution is a mixed integer programming approach for determining the minimal number of PMUs required to defend against an arbitrary set of unobservable attacks. The second is that the models for placing and selecting PMUs to detect k-sparse attacks are based on PMU capabilities; the relative merits of each capability in terms of the number of PMUs required to detect attacks are also discussed. The third contribution is that the models are tractable; this property is verified using empirical studies based on examples drawn from the power engineering literature.

2. Unobservable smart grid data integrity attacks

For completeness, we first summarize the main results in [9]. Electric power systems are potentially vulnerable to a large number of unobservable data integrity attacks. Data integrity attacks seek to modify data that is measured at remote locations (e.g., by meters and sensors) at sensing or during data transmission to other locations (e.g., control centers). Data integrity attacks that are consistent with power flow physics and do not involve compromised data are called unobservable attacks [14]. An unobservable attack requires coordination – compromised meter readings must be carefully orchestrated to fall in a low-dimensional manifold in order for the attack to be unobservable. Since the attacks are not observable, they can induce significant errors in state estimation and other applications. Interested readers are referred to [9,14] for formal treatments of unobservable attacks.

Because compromising large numbers of power grid sensors is a difficult task, this paper focuses on attacks that compromise a modest number of meters as discussed in [9]. It describes efficient algorithms that discover unobservable attacks involving the compromise of exactly two power injection meters and an arbitrary number of power meters on lines. This approach is used to enumerate sparse attacks. PMU resources are then optimized based on this set of attacks.

One of the interesting attributes of unobservable attacks is that they partition a power network into observable islands. The islands correspond to disjoint subsets of buses that share the same perceived change of state under attacks [9].

Fig. 1 shows an example of how an attack partitions a network into islands. Due to space constraints, the green rectangles group 265 and 18 buses. The grid in Fig. 1 is divided into three islands by the attack (red squares). Two PMUs in two different islands are sufficient as a countermeasure to the attack (e.g., buses 9026 and 9052). Conceptually, this means that the phase angles shift by the same amount in each island. A PMU in an island can detect if a shift is due to the normal behavior of the system or if it is only a perceived shift due to an attack. Thus, PMUs render the attack observable. As will be discussed later, during an attack, at most one island exhibits no shift. Giani et al. [9] have proposed the following definitions.

Definition 1. An attack $\alpha = (\mathbb{S}, a)$ is a set of meters $\mathbb{S}$ and an attack vector $0 \neq a \in \mathbb{R}^{m+n+1}$ where $n+1$ is the number of buses and m is the number of measurements. The nonzero components of a correspond to the compromised meters in $\mathbb{S}$, i.e., $k \in \mathbb{S} \iff a_k \neq 0$. Under the attack α, the meter readings