J Electr Eng Technol.2017; 12(1): 19-28
http://dx.doi.org/10.5370/JEET.2017.12.1.019

ISSN(Print) 1975-0102
ISSN(Online) 2093-7423

Protection Strategies Against False Data Injection Attacks with Uncertain Information on Electric Power Grids

Junhyung Bae*, Seonghun Lee, Young-Woo Kim*** and Jong-Hae Kim†**

Abstract – False data injection attacks have recently been introduced as one of important issues related to cyber-attacks on electric power grids. These attacks aim to compromise the readings of multiple power meters in order to mislead the operation and control centers. Recent studies have shown that if a malicious attacker has complete knowledge of the power grid topology and branch admittances, s/he can adjust the false data injection attack such that the attack remains undetected and successfully passes the bad data detection tests that are used in power system state estimation. In this paper, we investigate that a practical false data injection attack is essentially a cyber-attack with uncertain information due to the attackers lack of knowledge with respect to the power grid parameters because the attacker has limited physical access to electric facilities and limited resources to compromise meters. We mathematically formulated a method of identifying the most vulnerable locations to false data injection attack. Furthermore, we suggest minimum topology changes or phasor measurement units (PMUs) installation in the given power grids for mitigating such attacks and indicate a new security metrics that can compare different power grid topologies. The proposed metrics for performance is verified in standard IEEE 30-bus system. We show that the robustness of grids can be improved dramatically with minimum topology changes and low cost.

Keywords: Power system state estimation, False data injection attack, Cyber security, Topology changes, Phasor measurement unit

1. Introduction

Cyber-attacks have been increasingly viewed as an imminent threat to the modern power grid. As supervisory control and data acquisition (SCADA) systems become more sophisticated and inter-connected, the connection between the grid control networks and the administrative networks connected to Internet makes them highly susceptible to intrusions. Hackers may have already penetrated power grids and have left malicious codes behind, raising serious security concerns. For instance, the primary cause of the Northeast blackout of August 2003 was a malicious software code in the state estimator at a control center [1]. Such worm-like behavior aggravates the problem when compromised systems can cause extensive damage not only to power grids but also to other critical infrastructures.

Restructuring of the electric power industry has transformed state estimation from an important application into a critical one. It is a key function in modern energy management system (EMS) that provides a complete, consistent, and accurate database as an input to all other online applications including contingency analysis, optimal power flow, and economic dispatch. It analyses the information from a number of measurements at the control center and estimates the current system operating state. Conventional state estimators use a set of measurements to estimate bus voltage phasors in power grids. To date, these measurements were obtained only through a SCADA system, which gathers real-time measurements from remote terminal units (RTUs) installed in substations.

In current implementations of state estimation, bad data detection is designed to detect gross errors in the measurements based on high measurement redundancy. However, this method may fail in the presence of a false data injection attack by an intelligent attacker. Such an attack on SCADA systems affects the outcome of state estimation and further misleads the operation and control functions, possibly resulting in catastrophic consequences. It was shown in [2] that possible attacks could be denial-of-service (DoS) attacks on the RTUs, deception attacks on the communicated data through the communication network, or attacks directed to the SCADA master through the local area network (LAN). Some of the literature has already mentioned these problems, such as DoS attacks, replay attacks and false data injection attacks [3-5]. DoS attacks

† Corresponding Author: Dept. of Electronic and Electrical Engineering, Catholic University of Daegu, Korea. (kjhassk@cu.or.kr)
* Dept. of Information and Communication Engineering, DGIST, Korea. (baejunh@dgist.ac.kr)
** Convergence Research Center for Future Automotive Technology, DGIST, Korea. (shunlee@dgist.ac.kr)
*** Dept. of Daegu Research Center for Medical Devices and Green Energy, KIMM, Korea. (ywkim@kimm.re.kr)
Received: March 12, 2016 ; Accepted: July 26, 2016

are those in which the attacker can flood the communication network with arbitrary traffic to deny service to either the RTU or the control center. Replay attacks in which the attacker manipulates the status and measurements of the data the RTU is sending by hijacking the packets in transit from the RTU to the control center. False data injection attacks, which several researchers have discussed with respect to state estimation, are topology related attacks.

In this paper, the focus is on false data injection attacks against the power system state estimator. False data injection attacks were first proposed in [4]. These attacks can manipulate the outcome of state estimation in an arbitrary and predicted way through cooperatively modifying selected meters while avoiding bad data alarms in the control center. Intelligent attacks such as false data injection attacks, which are designed based on the knowledge of the target system and experience in power grid operation and control, can cause the most severe damage to power grids. With a complete knowledge of grid topology, a malicious attacker can easily construct false data injection attacks by modifying selected meters. As a result of the potential damage to power grids, false data injection attacks have attracted intensive attention and research interest.

A common assumption in most prior work, e.g., in [4], [9], and [10], is that the malicious attacker has perfect knowledge about the power grid topology. However, an important practical issue is when the attacker has non-perfect knowledge with respect to the power grid topology and branch admittance information. Therefore, in this paper, we identify the practical sparse attack, which is essentially a cyber-attack under uncertain information due to the malicious attacker's lack of knowledge of the power grid parameters because the attacker has limited physical access to most electric facilities and limited resources to compromise meters. Furthermore, we suggest protection strategies for minimum grid topology changes or PMU installation against such sparse attacks.

The organization of this paper is as follows. We present the related work in Section 2. The power system modeling, state estimation and false data injection attack is discussed in Section 3. In Section 4, we introduce to identify of most vulnerable locations against sparse attacks. The proposed protection strategies and security metrics are presented in Section 5. Finally, simulations on an IEEE 30-bus system illustrating the effectiveness of the proposed method are discussed in Section 6.

2. Related Works

Human-made false data injection attacks against power system state estimation were first studied in Liu et al. [4]. They showed that a malicious attacker can manipulate the outcome of state estimate while avoiding bad data detection. A key point of [4] was that a false data injection attack is not detectable if the attacker vector a is a linear combination of the column vectors of the Jacobian matrix H; i.e., $a = Hc$, where c can be any nonzero vector. According to [4], a false data injection attack can be easily constructed if an attacker gains access to the power grid configuration.

Various attack detection algorithms have been designed as follows. An undetectable false data injection attack motivates a Bayesian framework, which was first proposed in Kosut et al. [6]. The historical data can be used by the control center to track its belief state of the power system. Kosut et al. [7] used a graph theoretic approach to launch stealthy false data injection attacks. According to [7], a computationally efficient algorithm was derived to detect false data injection attacks using the generalized likelihood ratio test (GLRT) in the Bayesian framework. Huang et al. [8] and [9] proposed cumulative sum (CUSUM)-based quickest detection (QD) to study the tradeoff between the attack detection speed and performance.

The problem of defending a set of state variables was first studied in earlier work [10]. The authors proposed an arithmetic greedy algorithm that finds the minimum set of protected (or encrypted) meters by gradually expanding the set of state variables. However, the computational complexity of the greedy algorithm can be higher in large scale power grids. More relevant to our work is the paper of Bobba et al. [11] and Kim et al. [12] who investigated the use of a minimum set of encrypted meters to mitigate cyber-attacks using heuristic algorithms. Unfortunately, these protections are generally impossible in practice because the number of state variables in a real power grid is typically large. The grid designer's protection budget is very likely insufficient for perfect protection. Furthermore, these approaches only considered that the attacker has complete knowledge of power system. According to a recent research of Rahman et al. [13] and Liu et al. [14], the attacker's knowledge may be limited.

To address this problem, we suggest optimal protection strategies to increase the security level against a sparse attack with uncertain information.

3. Preliminaries

In this section, we introduce the power system model, the theory of power system state estimation and basic principle of false data injection attack.

3.1 System assumptions

In this paper, we assume that:

1) A power grids consist of active power flow measurements at all branches on both-ends (meaning that a power grid is an observable system);

2) A simplified linear approximation model is considered because [4] demonstrated that an adversary can inject false

data into state estimation that uses a DC power flow model;

3) Let m and n be the total number of measurements and states on the power grid ($m > n$).

3.2 Active power flow model

The given power grid has $n+1$ buses (including a reference bus). Here, we only consider a model consisting of active power flows P_{ij} and bus phase angles θ_i, where $i, j = 1, \dots, n+1$. Assuming that the resistance in the branch connecting buses i and j is smaller than its reactance, we have the active power flow model [15],

$$P_{ij} = \frac{V_i V_j}{X_{ij}} \sin(\theta_i - \theta_j) \tag{1}$$

where V_i is a voltage magnitude in bus i and X_{ij} is a reactance of the branch between bus i and j on power grid. If the voltage phase differences between two buses are sufficiently small and the voltage magnitudes are near unity, Eq. (1) can be further simplified as a linear relation, i.e.,

$$P_{ij} = \frac{1}{X_{ij}} (\theta_i - \theta_j) \tag{2}$$

3.3 State estimation

In the state estimation problem, we aim to estimate n phase angles given a set of m active power flow measurements. The voltage level of each bus as well as the reactance of each branch is assumed to be known.

For a given power grid, the linear model for active power flow measurements and bus phase angles can be expressed in the following form [11]:

$$z = Hx + e \tag{3}$$

where

$z \in \mathbb{R}^m$ meter measurements,
$H \in \mathbb{R}^{m \times n}$ Jacobian matrix,
$x \in \mathbb{R}^n$ bus phase angle θ_i and
$e \in \mathbb{R}^n$ measurement errors of zero-mean Gaussian variables with covariance matrix R, $\mathcal{N} \sim (0, R)$, $R = diag(\sigma_1^2, \sigma_2^2, \dots, \sigma_m^2)$ where σ is the variance of meter error.

If a measurement error follows the standard normal distribution and $m > n$ meaning that the system is over-determined, then the estimation problem can then be solved, as

$$\hat{x} = (H^T H)^{-1} H^T z \tag{4}$$

where $\hat{x}$ is estimated states.

3.4 Bad data detection

Generally, the bad data processing that is commonly used in state estimation is beneficial for power system application functions. Some meters can be corrupted by gross errors due to reasons such as incorrect configuration or failure of meters. Given an accurate system model, measurements with gross errors are expected to force the estimated state away from the true system state. Therefore, grid designers use statistical tests, called bad data detection, to detect, identify and remove measurements with gross errors [4].

The most commonly used approach to detect the presence of bad data in power systems is based on the $\mathcal{L}_2$-norm of measurement residuals. (A measurement residual is defined as the difference between the observed measurements and the estimated measurements.) In the control center, the presence of bad data is detected if the following condition is violated

$$\left\| z - H\hat{x} \right\| \le \tau \tag{5}$$

where τ is the detection threshold. If the residual is larger than expected, an alarm is triggered and the bad data is identified and removed.

3.5 False data injection attacks

Several scenarios of false data injection attacks on power grids were analyzed in [4]. The authors of [4] considered a linear model, in which were perfectly known by the attacker, and focused on attack policies that would guarantee the measurement residual to remain unchanged for the linear least-squares method.

The attacker's goal is either random or targeted attacks as follows: 1) a random attack in which the attacker aims to find any attack vector as long as it can result in a wrong estimation of state variables; 2) a targeted attack in which the attacker aims to find an attack vector that can inject a specific error into certain state variables. The targeted attack can potentially cause more damage to the system.

Besides describing the basic false data injection attacks, we also use two realistic attack constraints as follows: 1) limited access to meters and 2) limited resources available to compromise meters. Due to the first constraint, the attacker is restricted to accessing some specific meters because of physical protection devices. Due to the second constraint, the attacker is limited in the resources required to compromise meters. For example, the attacker only has resources to compromise up to k meters. Due to the limited resources constraint, the attacker may also want to minimize the number of meters to be compromised.

The authors of [4] developed a method for constructing an attack vector a. The theorem is that $a = Hc$ (where c is an arbitrarily-injected error) exists if and only if $Ba = 0$, where $B = I - H(H^T H)^{-1} H^T$, B is a residual sensitivity

matrix. Let $P = H(H^T H)^{-1} H^T$ where P is so-called a projection matrix. If the attacker can compromise specific k meters, where $k > m - n$, then there always exist attack vectors $a = Hc$ such that $a \neq 0$. In other words, if the attacker has access to information of H, s/he can launch a false data injection attack on power grids such that the resulting corrupted state can avoid being detected by the residual test.

Theorem in [4] shows that the malicious data $z^a = z + a$ can pass the bad data detection if a is a linear combination of the column vectors of H. As explained previously, we have $\|z - H\hat{x}\| \leq \tau$ where τ is the detection threshold that is pre-defined to control the tolerance of residuals. Let $\hat{x}^{bad}$ represent the estimated state variables when using the manipulated measurements z^a. Then, the $\hat{x}^{bad}$ can be expressed as $\hat{x} + c$. If $a = Hc$, then the resulting $\mathcal{L}_2$-norm of the residual is

$$\begin{aligned} \left\| z^a - H\hat{x}^{bad} \right\| &= \left\| z + a - H\left(\hat{x} + c\right) \right\| \\ &= \left\| z - H\hat{x} + a - Hc \right\| \\ &= \left\| z - H\hat{x} \right\| \leq \tau \end{aligned} \tag{6}$$

In the results, malicious data z^a can pass the bad data detection.

4. Identification of Vulnerable Locations to False Data Injection Attacks

In this section, we propose a method of identification of vulnerable locations to false data injection attacks, especially sparse attacks with uncertain information. We have designed a model assuming the attacker knows incomplete knowledge on the power grids. Then we show the impact of such attacks through an example bus system.

4.1 Identification of vulnerable locations

We explain how a false data injection attacks with perfect or uncertain information can be formulated. Then, we mathematically characterize a relation between an attack with perfect information and attack with uncertain information and show the impact of such an attack on power grids.

Let us denote the attacker's understanding of the matrix H as

$$H = YA \tag{7}$$

where Y is an $(m \times m)$ diagonal matrix of branch reactance information and A is an $(m \times n)$ connectivity binary information matrix. If the attacker has perfect information, then s/he can construct the attack vector a in the following form:

$$a = YAc \Leftrightarrow Ba = 0 \tag{8}$$

However, if the attacker does not know the branch reactance information, then s/he can construct the attack vector a' assuming $Y = I$, I is identify matrix:

$$a' = Ac \Leftrightarrow B'a' = 0 \tag{9}$$

where B' is a residual sensitivity matrix of A, i.e., $B' = I - A(A^T A)^{-1} A^T$. Therefore, we obtain a relation equation between a and a' as follows,

$$a = Ya' \Leftrightarrow a' = Y^{-1} a \tag{10}$$

It happens to consider two subspaces null space of B, i.e., $N(B)$ and null space of B', i.e., $N(B')$, not just one. We look at the attack vectors that belong to both subspaces.

Theorem 1: If $N(B)$ and $N(B')$ are both subspaces of sparse attack vector space, then so is their intersection $N(B) \cap N(B')$. The sparse attacks belonging to both spaces form another subspace.

Proof: Suppose sparse attack vector belongs to $N(B) \cap N(B')$, in other words, they are vectors in $N(B)$ and also in $N(B')$. The results of scalar multiplication stay within the intersection. Geometrically, the intersection of two regions is again a subspace. ■

The present study is motivated by the fact that an attacker would most likely use the sparest attack with uncertain information and corrupt as few meters as possible.

We introduce an example 5-bus system to explain Theorem 1 and the impact of such an attack vector. As an example, in the power grid model shown in Fig. 1 and Table 1, we obtain the following model in which the measurements consist of active power flows at all branches on both-ends. Note that the system observability is independent of the branch parameters as well as the operating state of the system [15]. First, if the attacker has uncertain power grid topology information, then s/he can construct the matrix A (12×4) as follows:

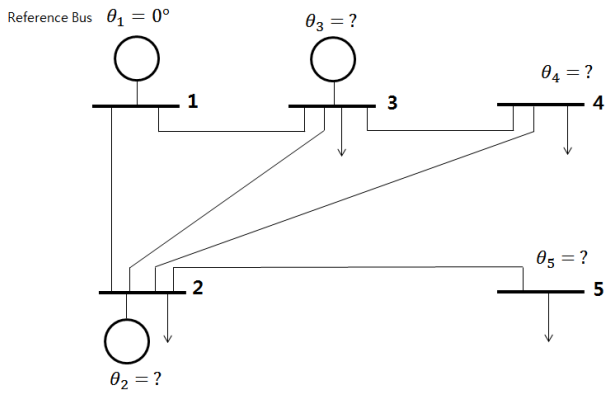


Fig. 1. Example 5-bus system

Table 1. Branch reactances of example 5-bus system

Branch connection	Branch reactance information
1-2	0.06
1-3	0.24
2-3	0.18
2-4	0.14
2-5	0.12
3-4	0.03

$$A=\begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ -1 & 0 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ -1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \end{pmatrix} \quad (11)$$

where $x=(\theta_2,\theta_3,\theta_4,\theta_5)^T$ and θ_1 is a reference bus phase angle. Note that the reference bus is typically excluded from states and the corresponding column doesn't exist in the matrix A. Here A^TA is invertible and it is possible to estimate the phase angles in the power grids. Now, the matrix B' (12×12) becomes

$$B'=\begin{pmatrix} 0.6875 & 0.3125 & \cdots & 0 & 0 & \cdots & 0.0625 \\ 0.3125 & 0.6875 & \cdots & 0 & 0 & \cdots & -0.0625 \\ -0.1875 & 0.1875 & \cdots & 0 & 0 & \cdots & -0.0625 \\ \vdots & \vdots & \ddots & \cdots & \cdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0.5 & 0.5 & \cdots & 0 \\ 0 & 0 & \cdots & 0.5 & 0.5 & \cdots & 0 \\ \vdots & \vdots & \ddots & \cdots & \cdots & \ddots & \vdots \\ 0.0625 & -0.0625 & \cdots & 0 & 0 & \cdots & 0.6875 \end{pmatrix} \quad (12)$$

Secondly, if the attacker has perfect power grid topology, then s/he can construct matrix H (12×4) as follows:

$$H=\begin{pmatrix} -16.6667 & 0 & 0 & 0 \\ 16.6667 & 0 & 0 & 0 \\ 0 & -4.1667 & 0 & 0 \\ 0 & 4.1667 & 0 & 0 \\ 5.5556 & -5.5556 & 0 & 0 \\ -5.5556 & 5.5556 & 0 & 0 \\ 7.1429 & 0 & -7.1429 & 0 \\ -7.1429 & 0 & 7.1429 & 0 \\ 8.3333 & 0 & 0 & -8.3333 \\ -8.3333 & 0 & 0 & 8.3333 \\ 0 & 33.3333 & -33.3333 & 0 \\ 0 & -33.3333 & 33.3333 & 0 \end{pmatrix} \quad (13)$$

Table 2. Original and manipulated phase angles

Bus index	Original (radian)	Manipulated (radian)
2	-0.0991	-0.0991
3	-0.0971	-0.0971
4	0.0530	0.0530
5	-0.2500	-0.3700

Now, the matrix B (12×12) becomes

$$B=\begin{pmatrix} 0.5244 & 0.4756 & \cdots & 0 & 0 & \cdots & 0.0075 \\ 0.4756 & 0.5244 & \cdots & 0 & 0 & \cdots & -0.0075 \\ -0.0976 & 0.0976 & \cdots & 0 & 0 & \cdots & -0.0299 \\ \vdots & \vdots & \ddots & \cdots & \cdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0.5 & 0.5 & \cdots & 0 \\ 0 & 0 & \cdots & 0.5 & 0.5 & \cdots & 0 \\ \vdots & \vdots & \ddots & \cdots & \cdots & \ddots & \vdots \\ 0.0075 & -0.0075 & \cdots & 0 & 0 & \cdots & 0.5108 \end{pmatrix} \quad (14)$$

Ideally, in order to reduce the cost of an attack, the attacker wants to compromise as few meters as possible [16]. From matrix B' and B one is led to believe that the most vulnerable meters, i.e., the meter measurements in branch 2-5, are sensitive to the sparsest attack. The attacker needs to find the sparsest attack vector satisfying $N(B)\cap N(B')$. For example, the attacker with uncertain information can represent a sparsest basis attack vector $a'=(0,0,0,0,0,0,0,0,1,-1,0,0)^T$. Let $B'=(b_1',b_2',\ldots,b_{12}')$ where b_l' $(1\le l\le 12)$ is the lth column vector of B'. Then,

$$B'a'=0\Leftrightarrow\left(b_1',b_2',\ldots,b_{12}'\right)\cdot(0,0,\ldots,1,-1,0,0)^T=0 \quad (15)$$

The lth elements being non-zero mean that the attacker compromises the meters, and then replaces its original measurement with a corrupted measurement. By launching these sparsest attacks, the attacker can manipulate the injected false data to bypass the bad data detection and also introduce arbitrary errors into the output of the state estimation as in Table 2. Table 2, which shows the original phase angles and phase angles manipulated by sparsest attack at branch 2-5 in Fig. 1.

5. Security Metrics for Performance Evaluation

In this section, we describe in detail our evaluation metrics. We thus propose here the metrics that considers the number of sparse attack solutions during the number of limited branch information knowledge.

5.1 Constraints for enhanced power grids

For a given grid, the power grid robustness could be

enhanced in several ways [17]. Adding branches without any restrictions until the sensitivity matrix B of power grid topology has a full rank would be an obvious one. However, for practical purposes, this method may be useless because, for example, the installation of branches would dramatically increase the cost and transmission losses. By associating cost to each branch of the grid, we need to seek a rebuilding solution that minimizes the total number of branches with meter measurements. Under these constraints, we propose the following protection strategies to mitigate false data injection attacks.

5.2 Protection strategies

5.2.1 Topology changes

In the given grid, we do the connections of branches, that is, the branches that connect a vulnerable bus with another bus, only if the robustness of the grid is increased. Note that a minimum change of the grid usually leads to a reconstruction of the attack vector solution. To choose optimal branch connections in various connection combinations, we define a degree of bus Γ_i where the number of branches connected to bus i. For example, in the 5-bus system in Fig. 1, the degrees of each buses are $\Gamma_i = \{2,4,3,2,1\}$. Therefore, we can obtain optimal robust power grid by connecting bus 4 and 5 because bus 4 is neighboring at bus 5 and it has relatively low measurement redundancy compared to other buses. If bus 4 and bus 5 are connected, we obtain the degree of bus $\Gamma_i = \{2,4,3,3,2\}$.

We propose here a security metrics that considers the number of sparse attack solutions during the number of limited branch information knowledge. The attack vectors can be chosen to be a linear combination of the vectors in the null space of the sensitivity matrix. However, such a set of possible linear combinations are not sparse compared to the basis vectors. Therefore, we consider that all possible choices of sparse attack lie in the basis vectors.

Table 3. Security metrics of given 5-bus system

No. of limited branch knowledge	Branch combinations for successful attack	No. of attack solutions
1	2-5	1
2	2-5 1-2, 1-3	2
3	2-5 1-2, 1-3 1-2, 2-3, 2-4 1-2, 2-3, 3-4	4

Table 4. Security metrics of topology changes (adding branch 4-5) 5-bus system

No. of limited branch knowledge	Branch combinations for successful attack	No. of attack solutions
1	0	0
2	1-2, 1-3	1
3	1-2, 1-3 1-2, 2-3, 3-4	2

Table 3 gives the simulation results on the given 5-bus system to show the performance evaluation metrics. In addition, Table 4 shows the performance evaluation of adding the branch 4-5. Table 4 is the metrics that characterize the tradeoff between the number of attack solutions versus the amount of limited branch information knowledge. These Tables illustrate the tradeoff faced by the attacker between increasing the amount of limited branch information knowledge and increasing the number of attack solutions. Furthermore, it shows that the robustness can be increased by adding the branch 4-5 at the given power grid topology. Our optimal grid is not only more robust against sparsest attacks, but also does not sharply increase the total number of branches without any loss of functionality.

5.2.2 PMUs installation

As described above, the addition of branches is not effective because of the high cost and practical installation constraints. As an alternative to providing protection for existing conventional meters, we consider the deployment of PMUs. By synchronizing to GPS time tag, PMUs have the capability of providing accurate synchronous phasor measurements for geographically dispersed buses on power grids [12]. In the linear model, a PMU installed on one bus can directly measure the bus voltage angle and branch currents. The PMU measurements are secure, because the real-time measured state vector on each bus represents the state of the power grid at each given instant. The measurements z_p consist of synchronized positive sequence voltage V_p and current I_p with zero-mean, normally distributed noise e_p [18].

$$z_p = \begin{pmatrix} V_p \\ I_p \end{pmatrix} + e_p \tag{16}$$

In reality, the system does not install enough PMU because of the high cost, the synchro-phasor need to be mixed with conventional meters $z_{mix} = [z \quad z_p]^T$.

By integrating PMUs into the process of state estimation, the redundant phasor measurement can improve the network observability and prevent false data injection attacks. The performance of bad data detection is related to the measurement redundancy, and by installing partial PMUs in identified vulnerable buses, the capability can be improved [19-22].

Table 5. Security metrics of PMU (at bus 5) installed 5-bus system

No. of limited branch knowledge	Branch combinations for successful attack	No. of attack solutions
1	0	0
2	0	0
3	1-3, 2-3, 2-4 1-3, 2-3, 3-4	2

Let us earlier example 5-bus system, assuming the voltage magnitudes $|V_i| = 1$, reactances $X_{ij} = 1$ in terms of attacker's viewpoint, we can obtain the following augmented model with installation of a PMU at bus 5,

$$A_{aug} = \begin{pmatrix} A \\ z_p \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ -1 & 0 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ -1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 1 \end{pmatrix} \quad (17)$$

where A_{aug} is augmented Jacobian with uncertain information. The augmented measurements are the phase angle at bus 5 and the current at branch 2-5. Then the matrix B'_{aug} of the augmented model becomes

$$B_{aug}{}' = \begin{pmatrix} 1.7468 & \cdots & 0.0633 & -0.0633 & \cdots & -0.0633 \\ 0.2532 & \cdots & -0.0633 & 0.0633 & \cdots & 0.0633 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0.0633 & \cdots & 1.7342 & 0.2658 & \cdots & 0.2658 \\ -0.0633 & \cdots & 0.2658 & 1.7342 & \cdots & -0.2658 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0.0506 & \cdots & -0.0127 & 0.0127 & \cdots & 0.0127 \\ 0.1899 & \cdots & 0.2025 & -0.2025 & \cdots & -0.2025 \\ -0.0633 & \cdots & 0.2658 & -0.2658 & \cdots & 1.7342 \end{pmatrix} \quad (18)$$

For false data injection attacks in the above example, we have shown that the attacker cannot always generate attack vectors to inject errors into estimates of state variables.

$$B'_{aug} a' \neq 0 \quad (19)$$

B'_{aug} has a full degree of redundancy and a full rank.

With these advantages, deploying a PMU at the bus 5 in Fig. 1, we can obtain the security metrics as given in Table 5.

6. Simulation Results

To validate the proposed method, we performed simulations on the standard IEEE 30-bus system as shown in Fig. 2. We use the configuration data of the test systems as obtained from the MATPOWER package [23]. For the test system, the state variables are the phase angles of the buses, and measurements are active power flows at all branches on both-ends when conventional meters are considered.

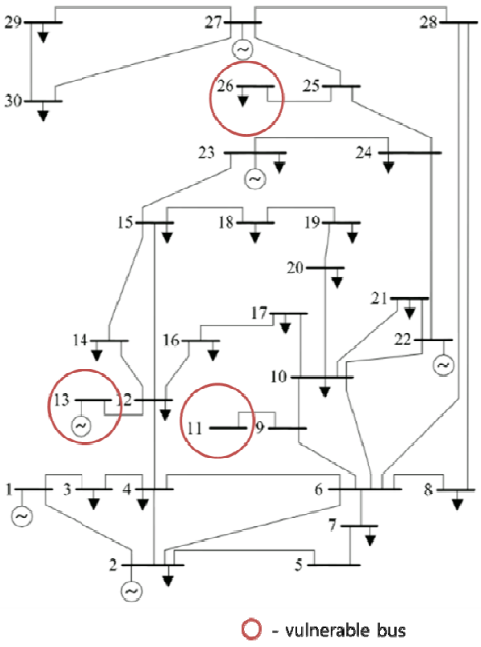


Fig. 2. Given IEEE 30-bus system

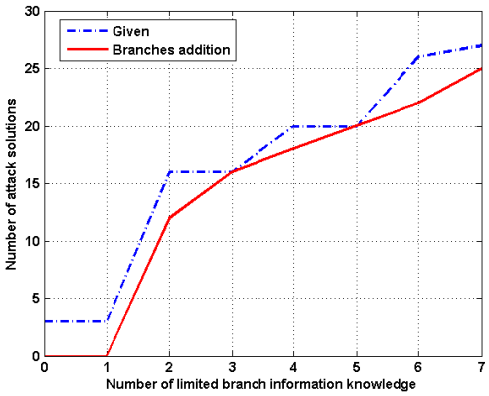


Fig. 3. Security metrics of the IEEE 30-bus system and topology changed system

Like process of the earlier 5-bus system, we confirmed the vulnerable buses 11, 13, and 26 on the IEEE 30-bus system by identifying rows of matrix B′. First, we have identified $\|B'\|_0$ and found attack vector $a' = Hc$ if and only if $B'a' = 0$. $\|B'\|_0$ denotes the number of non-zero elements in the residual sensitivity matrix. In Fig. 3, we plotted the security metrics for the given and topology changed system. The selective added branches are 11-16, 13-14, and 26-29 because the buses 16, 14, and 29 are neighboring buses and they have relatively low measurement redundancy. We can see that the number of attack solutions is 3 when the attacker does not know the branch information perfectly in the given system. However,

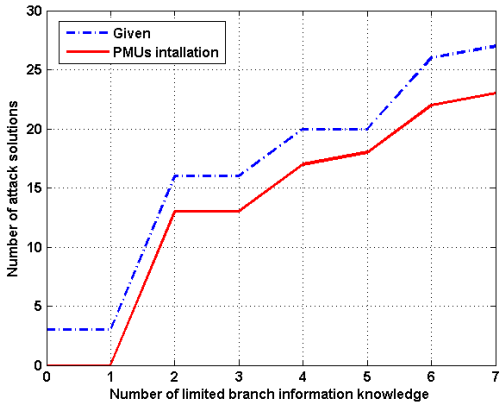


Fig. 4. Security metrics of the IEEE 30-bus system and the PMUs installed system

the number of attack solutions is 0 when the attacker does not know the branch information perfectly in the topology changed system. The number of attack solutions depends on the number of limited branch information knowledge as shown in Fig. 3. Clearly, if the attacker has branch information knowledge level increasingly, then the number of attack solutions can arbitrarily increase. In Fig. 4, we also plotted the security metrics for the given and PMU installed system. Like the topology changes approach, if the attacker has branch information knowledge level increasingly, then the number of attack solutions can arbitrarily increase. Interestingly, the security performance of PMU installed system is slightly better 8% than the performance of the topology changes. The deployment of PMUs made the secure power grid against cyber-attacks. As the concluding remarks, the proposed approaches made the power grid completely secure from sparsest attack with uncertain information because matrix B' has a full rank.

7. Conclusion

This paper has studied the problem of false data injection attacks on meters of electric power grids to manipulate state estimation results. In summary, the main contributions of this paper are as follows:

1) Firstly, it has identified a sparsest attack (or least-effort attack) is essentially an attack with uncertain information;
2) Secondly, it has mathematically formulated the relation between attacks with uncertain information and attacks with complete information and showed the impact of the attack on power grids;
3) Thirdly, it has suggested a security metrics that can compare given and various power grid topologies obtained by changing the minimum topology structure or PMU installation.

Finally, it has demonstrated on the standard IEEE 30-bus system that our strategies are more secure and economical for defending sparse false data injection attacks. The proposed methods can be used in the redesign of any power grid topology for cyber-security under various conditions.

Acknowledgements

This work was supported by the DGIST R&D Program of the Ministry of Science, ICT and Future Planning of Korea (16-RS-03).

References

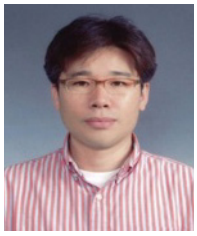
[1] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson and S. S. Sastry, "Cyber-security analysis of state estimators in electric power systems", *in Proc. IEEE Conf. Decision and Control*, Dec. 2010.
[2] A. Giani, S. S. Sastry, K. H. Johansson and H. Sandberg, "The VIKING Project: An initiative on resilient control of power networks", *in Proc. 2nd Int. Symp. Resilient Control Systems*, Idaho Falls, Idaho, pp. 31-35, Aug. 2009.
[3] Y. Mo and B. Sinopolo, "Secure control against replay attack", *in Proc. 47th Annual Allerton Conf.*, Monticello, IL, USA, pp. 911-918, Sep. 2009.
[4] Y. Liu, P. Ning and M. K. Reiter, "False data injection attacks against state estimation in electric power grids", *in Proc. 16th of ACM Conf. Computer and Communications Security*, Chicago, IL, pp. 21-32, Nov. 2009.
[5] A. Ashok and M. Govindarasu, "Cyber attacks on power system state estimation through topology errors", *in Proc. IEEE Power and Energy Society General Meeting*, San Diego, CA, pp. 1-8, Jul. 2012.
[6] O. Kosut, L. Jia, R. Thomas and L. Tong, "Limiting false data attacks on power system state estimation", *in Proc. 2010 Conf. Information Sciences and Systems (CISS)*, Princeton, NJ, pp. 1-6, Mar. 2010.
[7] O. Kosut, L. Jia, R. Thomas and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures", in Proc. IEEE Conf. Smart Grid Comm., Gathersburg, MD, pp. 220-225, Oct. 2010.
[8] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li and L. Song, "Bad data injection in smart grid: Attack and defense mechanisms", *IEEE Communications Magazine*, vol. 51, no. 1, pp. 27-33, Jan. 2013.
[9] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions", *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 106-115, Sept. 2012.

[10] S. Bi and Y. J. Zhang, "Defending mechanisms against false data injection attacks in the power system state estimation", *in Proc. IEEE Globecom Sg-Comnets*, Houston, TX, Dec. 2011.
[11] R. Bobba, K. Rogers, Q. Wang, H. Khurana, K. Nahrstedt and T. Overbye, "Detecting false data injection attacks on DC state estimation", *in Proc. 1st Workshop on Secure Control Syst.*, CPSWeek 2010, Stockholm, Sweden, Apr. 2010.
[12] T. T. Kim and H. V. Poor, "Strategy protection against data injection attacks on power grids", *IEEE Trans. Smart Grid*, vol. 3, no. 2, pp. 326-333, Jun. 2011.
[13] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids", *in Proc. IEEE Globecom,* Anaheim, CA, pp. 3153-3158, Dec. 2012.
[14] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information", *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1665-1676, Jul. 2014.
[15] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*, New York: CRCPress, 2004.
[16] A. Teieira, G. Dán, H. Sandberg and K. H. Johansson, "A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator", *in Proc. 18th Int. Federation of Automatic Control World Congress*, Milano, Italy, Aug. 2011.
[17] P. Chen, S. Cheng and K. Chen, "Smart attacks in smart grid communication networks", *IEEE Communications Magazine*, vol. 50, no. 8, pp. 24-29, Aug. 2012.
[18] Y. Huang, S. Werner, J. Huang, N. Kashyap and V. Gupta, "State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid", *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 33-43, Sep. 2012.
[19] A. G. Exposito and A. Abur, "Generalized observability analysis and measurement classification", *IEEE Trans. Power Systems*, vol. 13, no. 3, pp. 1090-1096, Aug. 1998.
[20] J. Chen and A. Abur, "Placement of PMUs to enable bad data detection in state estimation", *IEEE Trans. Power Systems*, vol. 21, no. 4, pp. 1608-1615, Nov. 2006.
[21] A. G. Phadke, J. S. Thorp, R. F. Nuqui and M. Zhou, "Recent developments in state estimation with phasor measurements", *in Proc. Power Systems Conference and Exposition, PSCE'09*, IEEE/PES, Mar. 2009.
[22] J. Lee, V. Centeno, J. S. Thorp and A. G. Phadke, "Synchronized phasor measurement applications in power systems", *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 20-27, Jun. 2010.
[23] R. D. Zimmerman, C. E. Murillo-Sanchez and R. J. Thomas, "MATPOWER steady-state operations, planning and analysis tools for power systems research and education", IEEE Trans. Power Systems, vol. 26, no. 1, pp. 12-19, Feb. 2011.

Junhyung Bae received the B.S. degree in electronic engineering and avionics from Korea Aerospace University, Goyang, Korea in 2004 and the M.S. degree in electrical engineering from Hanyang University, Seoul, Korea in 2006. From 2006 to 2010, he was a researcher at the Division of Advanced Industry Science and Technology, Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, Korea. In 2011, he worked as a senior researcher at Samsung Thales, Co., Ltd., Daejeon, Korea. He is currently a researcher at the Convergence Research Center for Future Automotive Technology, DGIST. He is also currently Ph. D. Candidate from the Dept. of Information and Communication Engineering, DGIST. His research interests are state estimation, control and fault diagnosis in industry.

Seonghun Lee received the B.S., M.S. and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, Korea in 1996, 1998 and 2007, respectively. From 1999 to 2002, he was a junior research engineer at Daewoo Precision Co. Ltd., Busan, Korea. Then, from 2002 to 2005, he was a senior research engineer at the Agency for Defense Development (ADD), Daejeon, Korea. He is currently a principal researcher at the Convergence Research Center for Future Automotive Technology, DGIST. His research interests are automotive embedded systems, modeling and simulation for electric vehicles.

Young-Woo Kim received the B.S. degree in electrical engineering from Yeungnam University, Gyeongsan, Korea in 1997 and the M.S. and Ph.D. degrees from Nagoya University, Nagoya, Japan in 2000 and 2004, respectively. He was with the Space Robotic Research Center, Toyota Technological Institute, Nagoya from 2004 to 2007. From 2007 to 2012, he had been with EcoTopia Science Institute, Nagoya University, as an Assistant Professor and Graduate School of Engineering, Nagoya University as a Designated Assistant Professor. Since 2012, he has been working for Korea Institute of Machinery and Materials (KIMM), Daegu, Korea. His research interests are the areas of human centered engineering and hybrid/nonlinear control theory.



Jong-Hae Kim received the M.S. and Ph.D. degrees in electrical engineering from Yeungnam University, Gyeongsan, Korea in 1996 and 1999, respectively. He also received the Ph.D. degree in electrical engineering from Nagoya University, Nagoya, Japan in 2005. From 2005 to 2012, he had been with fundamental technology group of elementary technology team, CDS division, Samsung Electro-Mechanics, Co., Ltd., as group leader. Since 2012, he has been an assistant professor with the Dept. of electronic and electrical engineering, Catholic University of Daegu, Gyeongsan, Korea. His research interests are the areas of AC-DC, DC-DC and DC-AC power conversion topology, power factor correction circuit, soft-switching converter topology, wireless power transfer, virtual reality and hybrid/nonlinear control theory. He won the best paper award from ICCAS in 2005.