J. Mod. Power Syst. Clean Energy (2016) 4(3):496–505
DOI 10.1007/s40565-016-0223-6

Impact analysis of false data injection attacks on power system static security assessment

Jiongcong CHEN[1,2], Gaoqi LIANG[3], Zexiang CAI[1], Chunchao HU[2], Yan XU[4], Fengji LUO[5], Junhua ZHAO[6]

Abstract Static security assessment (SSA) is an important procedure to ensure the static security of the power system. Researches recently show that cyber-attacks might be a critical hazard to the secure and economic operations of the power system. In this paper, the influences of false data injection attack (FDIA) on the power system SSA are studied. FDIA is a major kind of cyber-attacks that can inject malicious data into meters, cause false state estimation results, and evade being detected by bad data detection. It is firstly shown that the SSA results could be manipulated by launching a successful FDIA, which can lead to incorrect or unnecessary corrective actions. Then, two kinds of targeted scenarios are proposed, i.e., fake secure signal attack and fake insecure signal attack. The former attack will deceive the system operator to believe that the system operates in a secure condition when it is actually not. The latter attack will deceive the system operator to make corrective actions, such as generator rescheduling, load shedding, etc. when it is unnecessary and costly. The implementation of the proposed analysis is validated with the IEEE-39 benchmark system.

Keywords Cyber physical power system, Static security assessment, False data injection attacks, State estimation

1 Introduction

Ensuring the operation security of a power system has always been a basic yet important requirement. Security assessment is essential to monitor and control the power system in near real-time, and also one of the most important functions of Energy Management System (EMS) [1, 2]. Usually, it consists of static security assessment (SSA) and dynamic security assessment (DSA). The former one mainly focuses on branch overflow and bus overvoltage following a disturbance [3]. The latter one mainly focuses on the stability criteria (including rotor angle, voltage, and frequency) is

CrossCheck date: 20 June 2016

Received: 10 January 2016 / Accepted: 20 June 2016 / Published online: 25 July 2016

✉ Gaoqi LIANG
gaoqi.liang@uon.edu.au

Jiongcong CHEN
chenjiongcong_ee@163.com

Zexiang CAI
epzxcai@scut.edu.cn

Chunchao HU
hcc.1220@163.com

Yan XU
yan.xu@sydney.edu.au

Fengji LUO
fengji.luo@sydeny.edu.au

Junhua ZHAO
junhua.zhao@outlook.com

[1] School of Electric Power, South China University of Technology, Guangzhou, China

[2] Electric Power Research Institute of Guangdong Power Grid, Guangzhou, China

[3] Centre for Intelligent Electricity Networks, University of Newcastle, Newcastle, Australia

[4] School of Electrical and Information Engineering, University of Sydney, Sydney, Australia

[5] School of Civil Engineering, University of Sydney, Sydney, Australia

[6] School of Science & Engineering, Chinese University of Hong Kong (Shenzhen), Guangdong, China

violated when be subject to a disturbance [4–7]. In this paper, we focus on the SSA which highly depends on the state estimation results. Therefore, the accuracy of state estimation result is of high importance for the SSA and the corresponding security enhancement.

Researches recently show that due to the deeper integration of physical system and cyber system, the security and economy of the modern power system might be affected by cyber-attacks. Cyber-attacks have already made destructions to the control system. For example, in 2003, a cyber-attack penetrated a computer network at the Davis-Besse nuclear power plant in the U.S. While in 2010, the Stuxnet worm attacked Iran's Natanz nuclear fuel-enrichment facility [8]. The "BlackEnergy" worm has been confirmed of infecting multiple Ukrainian power substations in December, 2015. Around half of the homes in the Ivano-Frankivsk region in Ukraine were left without electricity for a few hours [9].

False data injection attack (FDIA) is a kind of cyber-attacks proposed by Liu *et al*. in 2009, which can make severely secure and economic impacts on the power system [10, 11]. Then, researches in FDIA-based cyber-attack have been extensive. Authors in [12] made a comprehensive review of state-of-the-art in FDIAs against modern power system. Liang *et al*. in [13] analyzed the physical consequences of FDIAs on the power system state estimation. Yu *et al*. [14] proposed a stealthy and blind attack without the knowledge of Jacobian matrix and any assumption about the distribution of stat variables. Hug *et al.* [15] studied the vulnerability assessment of FDIAs based on the AC state estimation model. Kim and Tong in [16] showed that the power system security and economy can be affected by the combination of topology attack and FDIA. The authors in [17–19] made their contributions on the impacts of FDIAs on electricity market, and proposed that FDIAs can make huge economic losses to the power market. Yuan *et al.* in [20] and [21] proposed that FDIAs can cheat the control center to do unnecessary load shedding to the power system which is a severely destruction to the system's economy and security. Yang *et al.* in [22] proposed a Polynomical-based compromise-resilient en-route filtering scheme to filter FDIAs effectively and achieve a high resilience to the number of compromised nodes without relying on static routes and node localization. Zhao *et al*. in [23] and [24] proposed a forecasting-aided implementation method to detect FDIA based on AC state estimation model. Chaojun *et al.* in [25] proposed a new detection method to detect FDIA by tracking the dynamics of measurement variations. Hao *et al.* in [26] proposed an efficient greedy search algorithm to quickly find subset of measurements to be protected to defend against FDIAs. Liu *et al*. in [27] expanded meters from the power side to the user side, and proposed an intrusion detection mechanism that can achieve collaborative detection of FDIA by setting spying domain randomly in physical memory in combination with using secret information and event log. From the literature, few researches focus on the impact analysis of FDIAs on the power system SSA. In this paper, we will analysis this problem based on nonlinear state estimation model which is more practical to the actual system operation.

As shown in Fig. 1, the security enhancement is implemented to the power system according to the SSA results. While, the SSA is based on the real-time system modeling and system monitoring. For modeling and monitoring, three types of measurements (i.e., the analog measurement, logic measurement, and pseudo- measurement) are gathered by Supervisory Control and Data Acquisition (SCADA) system and then transferred to other modules in EMS [28]. In EMS, topology processor is used to estimate the network topology; observability analysis represents that the power flow equations are solvable, which depends highly on the available measurements and their geographic distribution; and state estimation and bad data detection are used to estimate the state variables and filter raw data on the basis of redundant measurements [28]. Only when there is neither inconsistence between analog measurements and logic measurements, nor bad data signal shown in bad data detection module, can the estimated state variables be used in SSA and other higher layer applications afterwards.

In this paper, we intend to perform security and economy analysis of the SSA based on nonlinear power system model under FDIAs with transmission line real power flow overload/non-overload situations. We focus on the analog measurement manipulation situation. The manipulation of logic measurement, pseudo-measurement, and topology information is out of the research range of this paper. We intend to launch a successful FDIA that would evade being detected by the system and cause adverse SSA results compared to the actual situations. As a consequence, the corresponding security enhancement implemented by the system operator might be deceived to do unnecessary actions or do not do necessary actions to the power system.

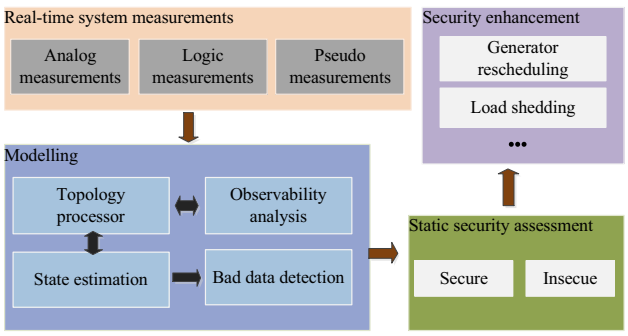

Fig. 1 Major processes of the online SSA

The major contributions of this paper are two-folds:

1) Analyze the influences of FDIAs on the SSA and show that the secure and insecure SSA results can be manipulated by the attacker;
2) Propose two targeted attack scenarios: fake secure signal attack and fake insecure signal attack. The former one is to convert the insecure situations into secure circumstances, in such a way that the control center is cheated to not do the necessary actions; the latter one is to convert the secure situations into insecure circumstances, in such a way that the control center is cheated to operate unnecessary actions.

This paper will be organized as follows. Section 2 introduces the basic theoretical background of launching a valid FDIA against state estimation based on linear and nonlinear model; Section 3 introduces the models and solving method of the proposed two targeted attack scenarios. Section 4 demonstrates the effectiveness of the proposed attack on IEEE benchmark system; Conclusions are drawn in Section 5.

2 Methodologies for FDIAs

In this section, the background of state estimation, bad data detection, and FDIA theory based on both linear and nonlinear power flow model are introduced.

2.1 Assumptions and preliminaries

This paper has the following assumptions:

1) The attacker has full knowledge of power topology information, system parameters, bad data detection strategy, etc.
2) The attacker is capable of falsifying any analog measurements that measured by meters.

Note that the above assumptions are commonly accepted in this research field [10–32], especially when the Ukrainian regional electric power distribution companies experienced cyber-attacks and caused serious blackouts on 23 December 2015.

2.2 State estimation and bad data detection

The state estimator provides estimated state variables (i.e., voltage and phase angle on each bus) based on a combination of meter measurements. The estimated state variables are the parameters that reflecting the operation conditions of the power system for a period of time [21].

Consider a power system with $n+1$ buses and m meters. The state estimation problem is to estimate the state variables $\boldsymbol{x} = (x_1, x_2, \cdots, x_n)^T$based on the meter measurements $\boldsymbol{z} = (z_1, z_2, \cdots, z_m)^T$, under the assumption that the measurement noise $\boldsymbol{e} = (e_1, e_2, \cdots, e_m)^T$ follows Gaussian distribution (0 mean and σ^2 covariance).

In linear power flow model, the state estimation model is formulated as

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{e} \tag{1}$$

where $\boldsymbol{H}$ is the Jacobian matrix, and $m > n$. Model (1) is commonly solved by weighted least squares (WLS) method by achieving the following optimization problem:

$$\min J(\boldsymbol{x}) = \frac{1}{2}(\boldsymbol{z} - \boldsymbol{H}\boldsymbol{x})^T \boldsymbol{W}(\boldsymbol{z} - \boldsymbol{H}\boldsymbol{x}) \tag{2}$$

where $\boldsymbol{W} = diag\{\sigma_1^{-2}, \sigma_2^{-2}, \cdots, \sigma_m^{-2}\}$. The solution can be computed in closed-form:

$$\hat{\boldsymbol{x}} = (\boldsymbol{H}^T\boldsymbol{W}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{W}\boldsymbol{z} \tag{3}$$

where $\boldsymbol{x} = [\hat{\boldsymbol{\theta}}, \hat{\boldsymbol{V}}]$ is the estimated state variable with $\hat{\boldsymbol{\theta}}$ as the phase angle and $\hat{\boldsymbol{V}}$ as the voltage magnitude.

In nonlinear power flow model, $\boldsymbol{h}(\boldsymbol{x})$ is used to denote the functional dependency between measurements and state variables. The model is then formulated as

$$\boldsymbol{z} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{e} \tag{4}$$

Then the corresponding optimization objective is:

$$\min \boldsymbol{J}(\boldsymbol{x}) = \frac{1}{2}(\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x}))^T W(\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})) \tag{5}$$

Due to the nonlinear relationship between measurement variables and state variables, it is difficult to have an analytical solution. Usually, iterative algorithm is applied to solve model in (4).

In bad data detection technique, the veracity of the estimated state variable is detected via the largest normalized residual (LNR) test, where the objective function $\boldsymbol{J}(\boldsymbol{x})$ is assumed to follow a chi-squared distribution with at most $m - n$ degrees of freedom, shown in Equation (6). τ is the threshold determined by a certain significance level.

$$J(\hat{\boldsymbol{x}}) < \tau \tag{6}$$

If (6) is satisfied, it shows the estimated state variable is capable of being used in higher layer applications; if not, the corresponding raw data should be filtered. The estimator should re-estimate the state variable until (6) is satisfied.

2.3 False data injection attack

FDIA is studied on both DC and AC model. In the linear model, the attacker fools the control center mainly by

keeping the measurement residual unchanged, although the attacker has injected bad data into meters.

Denoting $\boldsymbol{a}$ as the vector of malicious data which is injected into the original measurement data $\boldsymbol{z}$, therefore, the measurement vector is polluted as $\boldsymbol{z}_{bad} = \boldsymbol{z} + \boldsymbol{a}$ after attack. Denoting $\boldsymbol{c}$ as the deviation vector of the estimated state variable before and after the attack, the estimated state variable vector after attack can be represented as $\hat{\boldsymbol{x}}_{bad} = \hat{\boldsymbol{x}} + \boldsymbol{c}$, as shown in (7):

$$\begin{aligned}\hat{\boldsymbol{x}}_{bad} &= (\boldsymbol{H}^T\boldsymbol{W}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{W}\boldsymbol{z}_{bad} = (\boldsymbol{H}^T\boldsymbol{W}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{W}(\boldsymbol{z}+\boldsymbol{a}) \\ &= \hat{\boldsymbol{x}} + (\boldsymbol{H}^T\boldsymbol{W}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{W}\boldsymbol{a} = \hat{\boldsymbol{x}} + \boldsymbol{c}\end{aligned} \tag{7}$$

The target of the attacker is to find the vector of malicious data which keeps the measurement residual unchanged before and after attack. If $\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}$, then:

$$\begin{aligned}\left\|\boldsymbol{z}_{bad} - \boldsymbol{H}\hat{\boldsymbol{x}}_{bad}\right\| &= \left\|\boldsymbol{z} + \boldsymbol{a} - \boldsymbol{H}(\hat{\boldsymbol{x}} + (\boldsymbol{H}^T\boldsymbol{W}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{W}\boldsymbol{a})\right\| \\ &= \left\|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}} + (\boldsymbol{a} - \boldsymbol{H}(\boldsymbol{H}^T\boldsymbol{W}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{W}\boldsymbol{a})\right\| \\ &= \left\|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}} + (\boldsymbol{a} - \boldsymbol{H}\boldsymbol{c})\right\| = \left\|\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}\right\|\end{aligned} \tag{8}$$

In this way, the attacker can make a successful attack stealthily without being detected by bad data detection.

FDIA theory based on nonlinear model is much more complicated because the state variable and observation value has nonlinear relationship. The estimated state variable is gained through iteration algorithm. Therefore, it is much more difficult to find an analytical function to express the relationship between the malicious data and the system parameters. The key idea of AC model based FDIA is to find a vector of malicious data that makes the objective function after attack falls below the threshold as

$$J(\hat{\boldsymbol{x}}_{bad}) < \tau \tag{9}$$

3 SSA under FDIAs

FDIA is a harmful attack to the secure and economic operations of the whole power system because the estimated state variable used in all the higher layer applications in the control center is different from the actual one. More importantly, the control center will be cheated to believe the false estimated state variable. As a result, any operations based on the fake information will be implemented onto the actual system.

In this paper, the attacker's target is considered to make confusions of the estimated power flow on transmission lines based on the estimated state variable. In the SSA, if the calculated power flow on a transmission line is higher than the limit, it is considered as an insecure situation. The system operator should take some corrective actions, such as generator rescheduling, load shedding, etc. If no signal shows there is insecure situation of the entire system, it is considered as a secure situation. So, it is unnecessary for the system operator to do extra corrective actions. As shown in Fig. 2, there are four scenarios of the SSA when applying FDIAs into state estimation.

1) The actual SSA result shows the system is insecure, while it shows secure after attack;
2) The actual SSA result shows the system is secure, while it shows insecure after attack;
3) The actual SSA result shows the system is secure, while it shows secure after attack;
4) The actual SSA result shows the system is insecure, while it shows insecure after attack;

Apparently, the first and second scenarios are the most serious situations. We focus on these two scenarios in this paper and name them as fake secure signal attack and fake insecure signal attack respectively.

3.1 Fake secure signal attack

In fake secure signal attack, we focus on manipulating the fault condition into normal circumstance. In this scenario, open circuit fault condition is considered as the base case and causes overload situation. Shown as the first timeline in Fig. 3, the fault condition and state estimation procedure happen between two rounds of OPF. Once the online SSA shows insecure signal to the control center, the system operator will take corresponding actions immediately. However, when under attack, the attacker will deceive the state estimation and online SSA to show secure signal instead. As a consequence, necessary operations will not be taken then.

The mathematical model is formulated as:

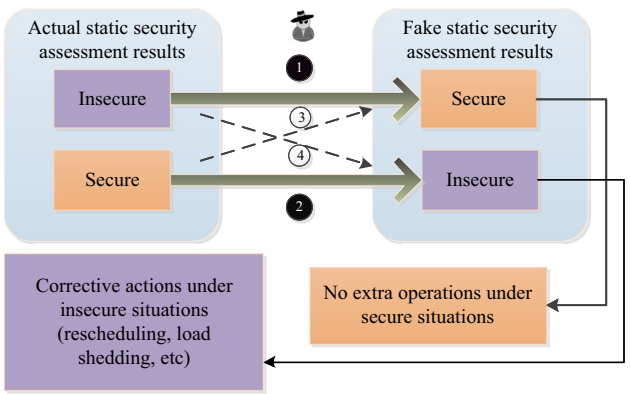

Fig. 2 Overview of the main purpose of FDIAs on the SSA

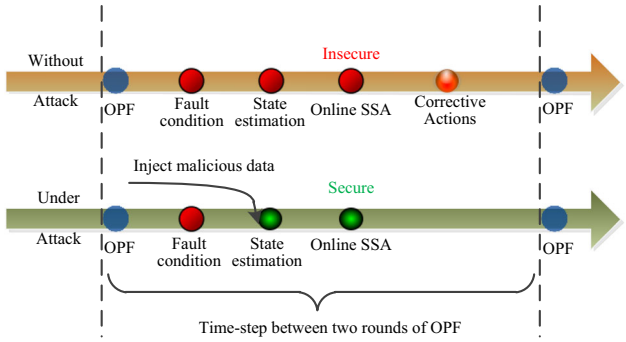

Fig. 3 Schematic diagram of fake secure signal attack

$$\min\|\boldsymbol{a}\|_0 \tag{10}$$

$$\text{s.t. } \boldsymbol{z}_{bad} = \boldsymbol{z} + \boldsymbol{a} \tag{11}$$

$$\boldsymbol{P}_{ij} = \boldsymbol{V}_i\boldsymbol{G}_{ij} + \boldsymbol{V}_i\boldsymbol{V}_j\left(\boldsymbol{G}_{ij}\cos\theta_{ij} + \boldsymbol{B}_{ij}\sin\theta_{ij}\right) \tag{12}$$

$$\boldsymbol{Q}_{ij} = \boldsymbol{V}_i\boldsymbol{B}_{ij} + \boldsymbol{V}_i\boldsymbol{V}_j\left(\boldsymbol{G}_{ij}\sin\theta_{ij} + \boldsymbol{B}_{ij}\cos\theta_{ij}\right) \tag{13}$$

$$\boldsymbol{P}_i = \boldsymbol{V}_i\sum_{j=1}^{n}\boldsymbol{V}_j\left(\boldsymbol{G}_{ij}\cos\theta_{ij} + \boldsymbol{B}_{ij}\sin\theta_{ij}\right) \tag{14}$$

$$\boldsymbol{Q}_i = \boldsymbol{V}_i\sum_{j=1}^{n}\boldsymbol{V}_j\left(\boldsymbol{G}_{ij}\sin\theta_{ij} + \boldsymbol{B}_{ij}\cos\theta_{ij}\right) \tag{15}$$

$$\boldsymbol{a}_{\min} < \boldsymbol{a} < \boldsymbol{a}_{\max} \tag{16}$$

$$[\boldsymbol{z}_{bad} - \boldsymbol{h}(\theta_{ij}, \boldsymbol{V}_i, \boldsymbol{V}_j)]^T\boldsymbol{W}[\boldsymbol{z}_{bad} - \boldsymbol{h}(\theta_{ij}, \boldsymbol{V}_i, \boldsymbol{V}_j)] < \tau \tag{17}$$

$$\boldsymbol{P}_{ij\min} < \boldsymbol{P}(\theta_{ij}, \boldsymbol{V}_i, \boldsymbol{V}_j) < \boldsymbol{P}_{ij\max} \tag{18}$$

$$\boldsymbol{Q}_{ij\min} < \boldsymbol{Q}(\theta_{ij}, \boldsymbol{V}_i, \boldsymbol{V}_j) < \boldsymbol{Q}_{ij\max} \tag{19}$$

where the measurement vector under no attack is expressed as $\boldsymbol{z} = [\boldsymbol{zP}_{ij}, \boldsymbol{zQ}_{ij}, \boldsymbol{zP}_i, \boldsymbol{zQ}_i]'$ which is composed of the real and reactive measurements from transmission lines and bus nodes, i.e., $\boldsymbol{zP}_{ij}$, $\boldsymbol{zQ}_{ij}$, $\boldsymbol{zP}_i$ and $\boldsymbol{zQ}_i$, respectively. The vector of malicious data is expressed as $\boldsymbol{a} = [\boldsymbol{z}\bar{\boldsymbol{P}}_{ij}, \boldsymbol{z}\bar{\boldsymbol{Q}}_{ij}, \boldsymbol{z}\bar{\boldsymbol{P}}_i, \boldsymbol{z}\bar{\boldsymbol{Q}}_i]'$ which is the corresponding injection values to the real and reactive measurements on transmission lines and bus nodes, i.e., $\boldsymbol{z}\bar{\boldsymbol{P}}_{ij}$, $\boldsymbol{z}\bar{\boldsymbol{Q}}_{ij}$, $\boldsymbol{z}\bar{\boldsymbol{P}}_i$ and $\boldsymbol{z}\bar{\boldsymbol{Q}}_i$, respectively.

Equation (10) is the objective to find the vector of malicious data $\boldsymbol{a}$ with minimum number of non-zero values which means the attacker will manipulate less meters to achieve his/her goal. (11)–(15) are the equality constraints; (11) shows that the vector of measurement used for state estimation is manipulated as $\boldsymbol{z}_{bad}$; (12)–(15) are the network equations with $\boldsymbol{P}_{ij}$ and $\boldsymbol{Q}_{ij}$ represent the power flow on transmission line, $\boldsymbol{P}_i$ and $\boldsymbol{Q}_i$ represent the power flow on bus i; θ_i,θ_j is the phase angle on node i; $\theta_{ij} = \theta_i - \theta_j$; $\boldsymbol{V}_i$, $\boldsymbol{V}_j$ are voltage magnitude on node i and node j; $\boldsymbol{G}_{ij}$ and $\boldsymbol{B}_{ij}$ are the real and imaginary part of admittance matrix on element ij;

Equation (16)–(19) are the inequality constraints; (16) is the constraint for the vector of malicious data $\boldsymbol{a}$ with $\boldsymbol{a}_{\min}$ and $\boldsymbol{a}_{\max}$ as the lower and upper boundary. In practical applications, the determinations of these boundary values can be determined by analyzing the historical operation data of the utility; (17) shows the bad data detection should be satisfied although the original measurements are manipulated; In (17), $\boldsymbol{h}(\theta_{ij}, \boldsymbol{V}_i, \boldsymbol{V}_j) = [\boldsymbol{P}_{ij}(\theta_{ij}, \boldsymbol{V}_i, \boldsymbol{V}_j), \boldsymbol{Q}_{ij}(\theta_{ij}, \boldsymbol{V}_i, \boldsymbol{V}_j), \boldsymbol{P}_i(\theta_{ij}, \boldsymbol{V}_i, \boldsymbol{V}_j), \boldsymbol{Q}_i(\theta_{ij}, \boldsymbol{V}_i, \boldsymbol{V}_j)]'$, $\boldsymbol{W}$is a diagonal matrix, τ is the bad data detection threshold; (18) and (19) show that the real and reactive power flow based on the estimated state variables on transmission lines should be within limit, with $\boldsymbol{P}_{ij\min}$, $\boldsymbol{Q}_{ij\min}$, $\boldsymbol{Q}_{ij\max}$ and $\boldsymbol{Q}_{ij\max}$ as the lower and upper boundary.

By solving the proposed mathematical model, the attacker can successfully convert the insecure signal into secure signal by injecting the malicious data $\boldsymbol{a}$. Since the necessary corrective actions are not taken, before operating the next round of OPF, the physical system may experience the following two kinds of situations:

Scenario 1: the overloaded transmission lines can survive for a period of time until the next round of OPF;

Scenario 2: the overloaded transmission lines cannot survive for a period of time until next round of OPF.

Apparently, scenario 2 is much more dangerous than scenario 1 because scenario 2 may cause chain reaction so that the system is pushed to an emergency condition, and may even cause blackout. As to which kind of influence the attack will make, depends on the specific network operation condition.

3.2 False insecure signal attack

In fake insecure signal attack, we focus on manipulating the normal situation into transmission line overload circumstance.

Shown as the first timeline in Fig. 4, the system operator will do nothing until the next round of OPF because the online SSA sends secure signal to the control center. However, when under attack, the secure condition is converted into insecure condition. As a consequence, firstly, the system operator will reschedule OPF immediately; secondly, based on the real-time monitoring by meters, the measurement values will be updated as the ones that reflect the condition after rescheduling. By re-estimating the system variable and redoing online SSA,if the SSA shows secure signal, the system operator will do nothing until the next round of OPF; otherwise, the system operator will believe that rescheduling is not helpful and will take corresponding actions according to the SSA result, mostly it will be the load shedding.

STATE GRID
STATE GRID ELECTRIC POWER RESEARCH INSTITUTE

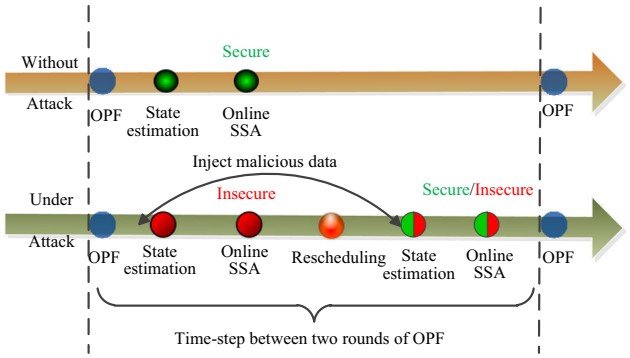

Fig. 4 Schematic diagram of fake insecure signal attack

Denoting the state estimation before rescheduling as the first round of state estimation, and the state estimation after re-scheduling as the second round of state estimation, whether the attacker injects malicious data into both rounds of state estimation depends on his/her purposes. In situation like this, the attacker will have the following two kinds of targets.

Target 1: The attacker launches fake insecure signal attack for the purpose of making the system operator do unnecessary rescheduling.

The attacker based on target 1 only need to focus on the first round of state estimation and online SSA. For injecting the appropriate malicious data that causes rescheduling, the mathematical model is formulated as

$$\min \|\boldsymbol{a}\|_0 \tag{20}$$

$$\text{s.t. Eq.}(11) \sim \text{Eq.}(17) \tag{21}$$

$$\exists \boldsymbol{P}_{ij} > \boldsymbol{P}_{ij\max},\ \boldsymbol{P}_{ij} \in \boldsymbol{P}_{ij}(\theta_{ij}, \boldsymbol{V}_i, \boldsymbol{V}_j) \tag{22}$$

where the explanation of (20) and (21) is similar with that of (10)–(17). (22) represents that as long as there is at least one calculated power flow out of limit, it is a valid attack. This model means by injecting the malicious data into original measurements, the SSA will always show that there is overloaded circumstance.

Target 2: The attacker launches fake insecure signal attack for the purpose of making the system operator perform unnecessary and costly load shedding.

Load shedding is a costly operation for the power grid. Usually, when the system is under the insecure situation, the operator would do re-scheduling to try to solve the problem. Only when re-scheduling does not work, load shedding is then taken as an emergency action to avoid the situation become worse. Different from target 1, target 2 requests the attacker has multiple injections. The attacker in this scenario not only needs to manipulate before the rescheduling, but also needs to manipulate after rescheduling. Normally, the attacker will solve model in (20)–(22) based on the measurement value after the first round of OPF, and solve model (20)–(22) again based on the updated measurement value after the rescheduling.

Shown in Fig. 4, the rescheduling is actually in between two rounds of OPF, followed by the second round of state estimation. The attacker should calculate the malicious data for the first and second round of state estimation based on the corresponding measurements. Therefore, by multiple injections, the attacker will successfully make the system take further corrective actions, i.e., load shedding.

Apparently, target 2 is much more dangerous to the power system than target 1 because implementing target 2 will cause costly load shedding. Usually, the system operator chooses to use the power transfer distribution factors (PTDFs) to determine the load shedding value for emergency measures. The PTDF is a sensitivity matrix that represents the sensitivities of branch flows to changes in nodal real power injections. The mathematical model is formulated as

$$\min \boldsymbol{c}(\Delta \boldsymbol{P}_D) \tag{23}$$

$$\text{s.t. } \Delta \boldsymbol{P}_{bus} = \Delta \boldsymbol{P}_D \tag{24}$$

$$\Delta \boldsymbol{P}_f = \boldsymbol{H}_{nbr\times nb} \Delta \boldsymbol{P}_{bus} \tag{25}$$

$$\boldsymbol{P}_{ij\min} < \boldsymbol{P}_{ij}(\theta_{ij}, \boldsymbol{V}_i, \boldsymbol{V}_j) - \Delta \boldsymbol{P}_f < \boldsymbol{P}_{ij\max} \tag{26}$$

where $\Delta \boldsymbol{P}_D$ is the vector of load shedding value; in (23), $\boldsymbol{c}(\cdot)$ represents the cost function of load shedding; usually, it is a linear relationship between the cost and the load shedding value; (24) refers to the energy imbalance equation when shedding load, i.e., the vector of the decreased injected power $\Delta \boldsymbol{P}_{bus}$ equals to the decreased load value $\Delta \boldsymbol{P}_D$; (25) is the PTDF sensitivity model for the change in the real power flow in branches given a unit decrease in the power injected node, where $\boldsymbol{H}_{nbr\times nb}$ is the PTDF sensitivity matrix, and $\Delta \boldsymbol{P}_f$ is the corresponding decreased power flow; (26) shows that the power flows after load shedding should still be within limits.

3.3 Solution method

For the proposed fake secure signal attack and fake insecure signal attack models, intelligence algorithms are usually used to find the solutions. In this paper, differential evolution (DE) method is used to solve this problem. DE method is a simple and efficient heuristic algorithm to optimize certain properties of a system by pertinently choosing the system parameters [32]. In this paper, by applying DE algorithm, we are interested in finding the appropriate malicious data which will neither lead to system unobservable nor be detected by bad data detection when adding malicious data to the meter measurements within iteration time.

4 Simulation results

In this section, we simulate the problems of FDIAs on the SSA on the modified IEEE-39 benchmark system. All simulation programs presented in this paper are implemented on MATLAB using MatPower. The IEEE-39 bus system has 10 generators and 46 branches. Each transmission line deploys a meter which measures the corresponding real and reactive power flows. The bad data detection threshold is set to be 70.993 (freedom $m - n = 46 \times 2 - 39$; $\alpha = 0.05$) in this paper. The maximum power flow on transmission lines is set to be 2 (p.u.).

Table 1 Demand parameters of the IEEE-39 benchmark system

Bus	Demand (MW)	Bus	Demand (MW)	Bus	Demand (MW)
1	100	14	–	27	70
2	–	15	80	28	50
3	100	16	80	29	70
4	155	17	–	30	–
5	–	18	80	31	50
6	–	19	–	32	–
7	80	20	200	33	–
8	150	21	80	34	–
9	50	22	–	35	–
10	–	23	80	36	–
11	–	24	80	37	–
12	80	25	80	38	–
13	–	26	30	39	100

Table 2 Differential evolution parameter setting for solving the models

Population size	100
Maximum iteration time	100
F	0.9
Cr	0.1

Table 1 shows the load value used by the OPF dispatch during this period of time. Table 2 is the DE parameter setting for solving the problem.

4.1 False secure signal attacks

In the case of fake secure signal attacks, the open circuit fault condition is assumed to happen on the 30th transmission line in IEEE-39 bus system.

With the demand value provided in Table 1, some of the actual power flows on transmission lines exceed the limit because of the fault condition, shown as the orange bar in Fig. 5. It is clearly seen that the open circuit fault condition causes overload on transmission line 3 and 25. When under no attack, the online SSA will immediately react to the situation and send insecure signal to control center. Then, control center will take corrective actions.

However, by injecting malicious data into the original measurements, the overloaded situation is manipulated within limit shown as the blue bar in Fig. 5. It is clearly seen that no line is in overload situation. Since the real power flow overload situation is of the most concern, we only compare the real power flow on transmission lines in this paper. Shown in Fig. 6, the orange bar represents the original real power flow measurements on transmission lines, while the blue bar represents the corresponding injection data. Consequently, the control center will do nothing during this period of time.

4.2 False insecure signal attacks

In the case of fake insecure signal attack, no matter the attacker's target is to make system do rescheduling or load shedding, he/she needs to manipulate the normal situation to overload situation by solving Equation (20)–Equation (22) based on the corresponding measurements. For the IEEE-39 bus system, the original real power flow measurements on transmission lines before re-scheduling

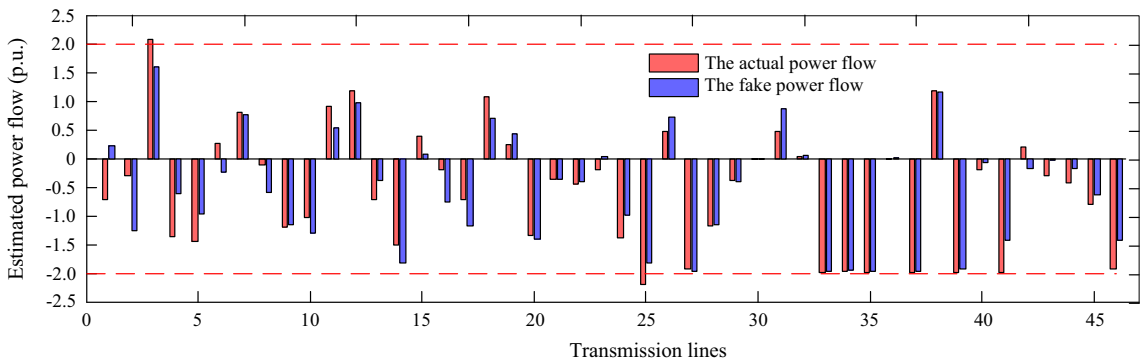

Fig. 5 State estimation result with and without attack (fake secure signal attack)

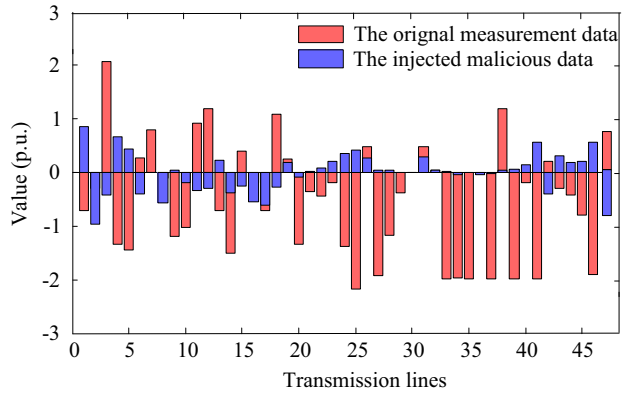

Fig. 6 Measurement data and injection data (fake secure signal attack)

are the values shown as the orange bar in Fig. 7. Then the state estimation calculates the corresponding state variables. As a consequence, the calculated power flow values are shown as the orange bar Fig. 8. It is clearly seen that the system is operating in good condition.

However, by injecting malicious data (blue bar in Fig. 7) into the original real power flow measurement on transmission lines, the attacker causes fake overloaded situations shown as the blue bar in Fig. 8. It is clearly seen from Fig. 8 that the secure situation is converted into

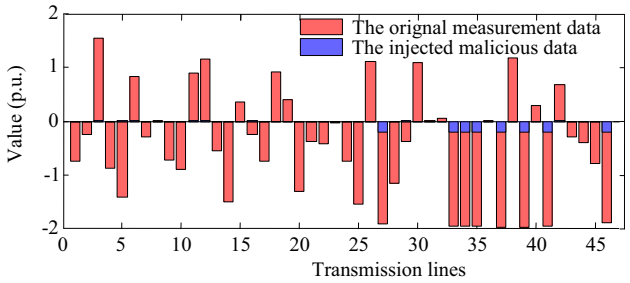

Fig. 7 Measurement data and injection data (fake insecure signal attack)

insecure situation with overload situation on transmission line 27, 33, 34, 35, 37, 39, 41 and 46.

Based on the insecure signal sent by the online SSA, the control center will do rescheduling. As discussed in Section 3, the attacker calculates the malicious data by solving (20)–(22) using the updated measurements, then injects malicious data after rescheduling. Load shedding is then implemented as an emergency measure. As shown in Table 3, the load shedding value for the IEEE-39 bus system is displayed, which is also calculated using DE algorithm. It can be seen from Table 3 that the total load shedding value is 123.65 MW. The unit load shedding cost is set to be 3.00×10^4 \$/MW. Therefore, it

Table 3 The load shedding value of the IEEE-39 benchmark system

Bus	Value (MW)	Bus	Value (MW)
1	4.20	21	14.04
2	–	22	–
3	0	23	34.41
4	0	24	2.14
5	–	25	7.65
6	–	26	9.36
7	0	27	20.45
8	0	28	13.06
9	0	29	0
10	–	30	–
11	–	31	0
12	0	32	–
13	–	33	–
14	–	34	–
15	0	35	–
16	5.61	36	–
17	–	37	–
18	0	38	–
19	–	39	0
20	12.71		

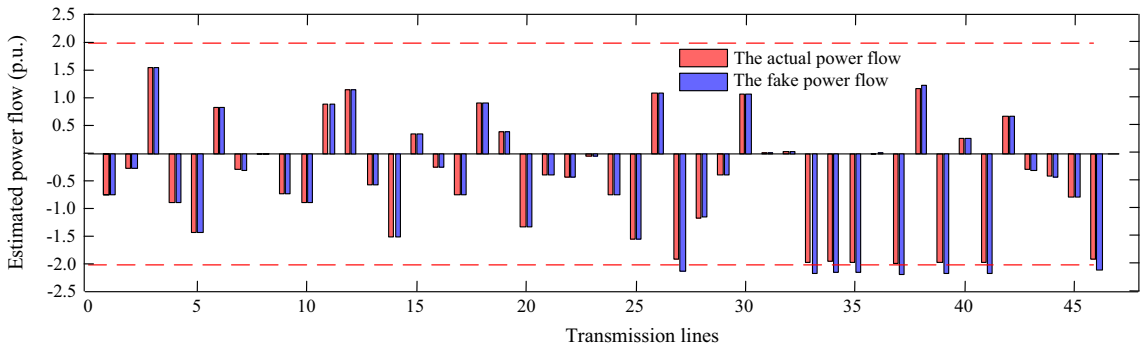

Fig. 8 State estimation result with and without attack (fake insecure signal attack)

takes the power system 3.71×10^6 $ as the extra increased cost which is actually unnecessary at all.

5 Conclusions

The cyber-attack is a harmful threat to the security and economy of modern power system. This paper analyzes the influences of FDIA, which is a kind of cyber-attack, on the SSA based on nonlinear power flow model. It shows that the attacker can make confusions of the secure and insecure signal to the control center by injecting malicious data into meter measurements. The system operator is therefore operating based on the false information which would make economic losses and may even lead to blackouts. Therefore, researches on how will cyber-attacks manipulate the power system and what influences will cyber-attacks make to the power system would have significant importance to enhance power system security.

Acknowledgment This work was supported by the Hong Kong Polytechnic University (1-YW1Q).

References

[1] Morison K, Wang L, Kundur P (2004) Power system security assessment. IEEE Power Energy Mag 2(5):30–39
[2] Wang L, Morison K (2006) Implementation of online security assessment. IEEE Power Energy Mag 4(5):46–59
[3] Saeh IS, Khairuddin A (2008) Static security assessment using artificial neural network. In: Proceedings of the IEEE 2nd international power and energy conference (PECON'08), Johor Baharu, 1–3 Dec 2008, pp 1172–1178
[4] Xu Y, Dong ZY, Zhao JH et al (2012) A reliable intelligent system for real-time dynamic security assessment of power systems. IEEE Trans Power Syst 27(3):1253–1263
[5] Xu Y, Dong ZY, Meng K et al (2011) Real-time transient stability assessment model using extreme learning machine. IET Gener Transm Distrib 5(3):314–322
[6] Dai Y, Xu Y, Dong ZY et al (2012) Real-time prediction of event-driven load shedding for frequency stability enhancement of power systems. IET Gener Transm Distrib 6(9):914–921
[7] Xu Y (2013) Dynamic security assessment and control of modern power systems using intelligent system technologies. Ph D Thesis, The University of Newcastle, Newcastle
[8] Stuxnet. http://en.wikipedia.org/wiki/Stuxnet. Accessed 16 May 2016
[9] Cyber-attack against Ukrainian critical infrastructure, Alert (IR-ALERT-H-16-056-01) (2016) The Industrial Control Systems—Cyber Emergency Response Team (ICS-CERT), Department of Homeland Security, Washington, DC
[10] Liu Y, Ning P, Reiter MK (2009) False data injection attacks against state estimation in electric power grids. In: Proceedings of the 16th ACM conference on computer and communications security (CCS'09), Chicago, IL, 9–13 Nov 2009, 12 pp
[11] Liu Y, Ning P, Reiter MK (2011) False data injection attacks against state estimation in electric power grids. ACM Trans Inf Syst Secur 14(1): Article 13/1-33
[12] Liang GQ, Zhao JH, Luo FJ et al (2016) A review of false data injection attacks against modern power systems. IEEE Trans Smart Grid. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7438916
[13] Liang JW, Sankar L, Kosut O (2016) Vulnerability analysis and consequences of false data injection attack on power system state estimation. IEEE Trans Power Syst. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7366616
[14] Yu ZH, Chin WL (2015) Blind false data injection attack using PCA approximation method in smart grid. IEEE Trans Smart Grid 6(3):1219–1226
[15] Hug G, Giampapa JA (2012) Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. IEEE Trans Smart Grid 3(3):1362–1370
[16] Kim J, Tong L (2013) On topology attack of a smart grid: undetectable attacks and countermeasures. IEEE J Sel Area Commun 31(7):1294–1305
[17] Xie L, Mo YL, Sinopoli B (2011) Integrity data attacks in power market operations. IEEE Trans Smart Grid 2(4):659–666
[18] Jia LY, Kim J, Thomas RJ et al (2014) Impact of data quality on real-time locational marginal price. IEEE Trans Power Syst 29(2):627–636
[19] Choi DH, Xie L (2013) Impact analysis of locational marginal price subject to power system topology errors. In: Proceedings of the 2013 IEEE international conference on smart grid communications, Vancouver, 21–24 Oct 2013, pp 55–60
[20] Yuan YL, Li ZY, Ren K (2011) Modeling load redistribution attacks in power systems. IEEE Trans Smart Grid 2(2):382–390
[21] Yuan YL, Li ZY, Ren K (2012) Quantitative analysis of load redistribution attacks in power systems. IEEE Trans Parallel Distrib Syst 23(9):1731–1738
[22] Yang XY, Lin J, Yu W et al (2015) A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems. IEEE Trans Comput 64(1):4–18
[23] Zhao JB, Zhang GX, Dong ZY et al (2016) Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation. IEEE Trans Smart Grid 7(1):6–8
[24] Zhao JB, Zhang GX, La Scala M, et al (2015) Short-term state forecasting-aided method for detection of smart grid general false data injection attacks. IEEE Trans Smart Grid. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7313024
[25] Gu CJ, Jirutitjaroen P, Motani M (2015) Detecting false data injection attacks in AC state estimation. IEEE Trans Smart Grid 6(5):2476–2483
[26] Hao JP, Piechochki RJ, Kaleshi D et al (2015) Sparse malicious false data injection attacks and defense mechanisms in smart grids. IEEE Trans Ind Inform 11(5):1198–1209
[27] Liu XX, Zhu PD, Zhang Y et al (2015) A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. IEEE Trans Smart Grid 6(5):2435–2443
[28] Balu N, Bertram T, Bose A et al (1992) On-line power system security analysis. Proc IEEE 80(2):262–282
[29] Kosut O, Jia LY, Thomas RJ et al (2011) Malicious data attacks on the smart grid. IEEE Trans Smart Grid 2(4):645–658
[30] Yang QY, Yang J, Yu W et al (2014) On false data-injection attacks against power system state estimation: Modeling and countermeasures. IEEE Trans Parall Distrib Syst 25(3):717–729

STATE GRID
STATE GRID ELECTRIC POWER RESEARCH INSTITUTE

[31] Liu X, Bao Z, Lu D et al (2015) Modeling of local false data injection attacks with reduced network information. IEEE Trans Smart Grid 6(4):1686–1696
[32] Storn R, Price K (1997) Differential evolution—a simple and efficient heuristic for global optimization over continuous spaces. J Glob Optim 11(4):341–359

Jiongcong CHEN is a Ph.D. student of South China University of Technology. Meanwhile, he is working in Smart Grid Department of Electric Power Research Institute of Guangdong Power Grid Co. Ltd. His interests are smart grid and renewable energy.

Gaoqi LIANG obtained the BS in automation from the North China Electric Power University, Baoding, China, in 2012. She is currently towards her Ph.D. degree in electrical engineering from the University of Newcastle, Australia. Her research interests include cyber physical system and its security.

Zexiang CAI obtained his Ph.D. from Tsinghua University in 1991. He has been a professor of the School of Electrical Power Engineering of South China University of Technology since 1998. His research interests are power system protection relay, power system stability and control.

Chunchao HU obtained his MS in electric engineering in 2011. He is now working in Smart Grid Department of Electric Power Research Institute of Guangdong Power Grid Co. Ltd. his research interests include smart grid and power market.

Yan XU obtained his Ph.D. from University of Newcastle in 2013. He is now with University of Sydney, Australia. His research interests include power system security and control.

Fengji LUO obtained his BS and MS in software engineering from Chongqing University, Chongqing, China, in 2006 and 2009, respectively. He received his Ph.D. in electrical engineering from the University of Newcastle, Australia, in 2013. Currently, he is a postdoctoral researcher with the University of Sydney, Australia. His research interests include demand side management, computational intelligence, distributed computing, and renewable energy.

Junhua ZHAO obtained his Ph.D. from the University of Queensland, Australia. He is with the Chinese University of Hong Kong (Shenzhen), Shenzhen, China, and also with the Electric Power Research Institute, CSG, Guangzhou, China. His research interests include power system analysis and computation, smart grid, cyber physical system, electricity market, data mining and its applications.