Future Generation Computer Systems 49 (2015) 94–103

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

# Abnormal traffic-indexed state estimation: A cyber–physical fusion approach for Smart Grid attack detection

Ting Liu *, Yanan Sun, Yang Liu, Yuhong Gui, Yucheng Zhao, Dai Wang, Chao Shen

*Ministry of Education Key Lab for Intelligent Networks and Network Security, School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi, China*

ARTICLE INFO

*Article history:*
Received 26 February 2014
Received in revised form
11 September 2014
Accepted 1 October 2014
Available online 12 October 2014

*Keywords:*
Smart grid
Security
Cyber–physical fusion
Bad data injection
Attack detection
Abnormal traffic-indexed state estimation

ABSTRACT

Integration with information network not only facilitates Smart Grid with many unprecedented features, but also introduces many new security issues, such as false data injection and system intrusion. One of the biggest challenges in Smart Grid attack detection is how to fuse the heterogeneous data from the power system and information network. In this paper, a novel cyber–physical fusion approach is proposed to detect a Smart Grid attack Bad Data Injection (BDI), by merging both the features of the traffic flow in information network and the inherent physical laws in the power system into a unified model, named as Abnormal Traffic-indexed State Estimation (ATSE). The cyber security incidents, monitored by intrusion detection system (IDS), are quantized to serve as the impact factors that are incorporated into the bad data detection system based on state estimation model in power grid. Hundreds of attack cases are simulated on each transmission line of three IEEE standard systems to compare ATSE with current cyber, physical abnormal detection methods and cyber–physical fusion method, including IDS (Snort), bad data detection algorithm (Chi-square test) and SCPSE. The results indicate that ATSE can improve the detection rate 20% than the Chi-square Test on average, filter most false alarms generated by Snort, and solve the observability problem of SCPSE.

## 1. Introduction

Emerging as the combination of information network and traditional power grid, Smart Grid empowers today's power system with a wealth of unprecedented features such as observability, controllability, resilience, robustness and self-healing [1]. However, a new plethora of security issues arises from increased dependency on the highly interconnected and open information networks which are applied to transmit the state measurement, pricing information and control actions, etc. Various attacks, such as information tampering and system intrusion, would impose serious threat on security and stability of Smart Grid. For example, vandalistic hackers can launch attacks, such as denial of services, measurement revision and malicious control command injection, to penetrate communication process, steal user privacy and even compromise the control system, which may cause devastating disruptions on the critical power plant and lead to catastrophic consequence on the crucial power infrastructure [2–4]. All of these attacks present a new feature, that is, intruding and hijacking the physical system from the information network. In this paper, we focus on how to detect Bad Data Injection (BDI) which intrudes the Smart Grids communication network and injects a well-constructed data to bypass current Bad Data Detection system in power system [5,6].

Guaranteeing the system availability and reliability of Smart Grid in the face of various malicious attacks is a challenging task. Built upon the existing power infrastructure, Smart Grid is largely dependent on the legacy systems that are not initially designed to be attack resilient. Several potential cyber threats to Supervisory Control And Data Acquisition (SCADA) system have already been categorized and assessed [3,7]. The increasing use of open architecture and the mainstream trend of becoming networked make traditional grid more error prone from cyber attacks, adding chance of system failure and malfunctions. Thus, the inherent vulnerabilities of the legacy power system as well as a wide range of new security risks added due to the integration of cyber network, raise profound dilemmas for Smart Grid security. The complex, large-scale and highly interconnected cyber–physical system makes it inadequate to directly apply existing solutions to address the security challenges in Smart Grid [8].

* Corresponding author.
*E-mail addresses:* tliu@sei.xjtu.edu.cn (T. Liu), ynsun@sei.xjtu.edu.cn (Y. Sun), yliu@sei.xjtu.edu.cn (Y. Liu), yhgui@sei.xjtu.edu.cn (Y. Gui), yczhao@sei.xjtu.edu.cn (Y. Zhao), daiwang@sei.xjtu.edu.cn (D. Wang), cshen@sei.xjtu.edu.cn (C. Shen).

http://dx.doi.org/10.1016/j.future.2014.10.002
0167-739X/© 2014 Elsevier B.V. All rights reserved.

For the cyber system, the current approaches, including various network-based and host-based security technologies, are not appropriate to monitor the communication in industrial control networks. These existing network-based solutions, such as traffic analysis and intrusion detection, are generally not equipped to support analysis of protocols adopted in power system, which cannot be directly applied to interpret the power data and parameters. Moreover, the high false positive rate is a big issue for most cyber defense techniques. It would be of great difficulty for operators to identify and locate real attacks from a huge amount of false alarms. The host-based technologies, such as access control, file monitoring, anti-virus and Sandbox have to be installed on the device. Since millions of meters and Remote Terminal Units (RTUs) in the power system are unable to install software, it is an astronomical cost to replace these wide-spread devices and update the security system regularly.

As to the power system, the measurement errors need to be taken into consideration for those traditional solutions that utilize the physical restrictions to model power system for data consistency check. Yet, this error-tolerance conversely provides a tool for malicious attackers to inject elaborately designed bad data that cannot be detected, which indicates the intrinsic drawbacks of the methods based on physical laws [9]. Recent works demonstrate that the adversary, armed with the knowledge of the power system topology and real-time measurements, can construct a false data injection attack without triggering the bad data detection system in power system [5,10]. Besides, the cyber impact is barely considered in the physical model. Thus, it is difficult to ensure the integrity and confidentiality of power system data and the validity of the control command.

Moreover, the tight coupling between the physical systems and the information networks creates a completely new attack route for adversaries, that is, penetrate the information network to compromise the Smart Grid. Various incidents, such as Stuxnet attack on Iran's Bushehr nuclear power station, demonstrate that cyber intrusions could cause severe consequences on critical physical infrastructure [7].

Fusion is considered to be an optimal solution for attack detection in Smart Grid, especially meaningful for the hybrid cyber–physical attack that will lead to the interactive reaction in both information network and power system [11]. However, how to fuse the information from the cyber and physical side is quite challenging, which mainly faces the following three difficulties:

(1) *Heterogeneous cyber and physical data*. The classical physical system is usually modeled in the form of continuous differential equations, subjected to certain boundary conditions and conformed to time–space continuum. Yet, the cyber network is commonly characterized based on the discrete mathematics, experiences and cognition, which focuses on the implementation of system functionality and takes no account of the continuous time and space. The first challenge of Smart Grid attack detection is how to unify the clearly structured physical data and the loosely organized cyber data.

(2) *Multi-source data*. The data in Smart Grid are collected from millions of smart meters, intelligent appliances and distributed storage devices. The relationship model of these data is high-dimensional and complex. Moreover, it is particularly difficult to abstract and quantify them from the dynamic, complex and highly inter-connected cyber–physical system.

(3) *Security model of Smart Grid*. The model for security requirement and attack behavior is the basis of security monitoring and defense. The security model of Smart Grid should consider both the physical restrictions from the power grid and the possible cyber impact imposed on the physical system, which may have diverse and distinct requirement regarding security needs. This also becomes a major obstacle to establish a reliable security model for Smart Grid.

This study proposes a novel cyber–physical fusion approach by developing an abnormal traffic-indexed state estimation (ATSE) method for attack detection in Smart Grid, merging both the traffic flow of the information network and the physical laws inherent in power system into a unified model. The cyber security incidents are quantized to serve as the impact factors that are fused into the state estimation model in power system. Specifically, the abnormal traffic in cyber network are quantified according to the logs associated with the device-IP map, attack type and threat priority. The cyber impact factors are applied to reduce the influence of the measurements from suspicious sources in the state estimation. Thus the difference between the estimated results and real states would be decreased, and the residuals between estimated results and measurements on compromised devices would be increased. Traverse attacks are conducted on each transmission line of three IEEE standard systems, 14-bus, 39-bus and 118-bus. ATSE and two well-known detection methods are applied to detect the attacks, including IDS (Snort) and bad data detection algorithm (Chi-square test). The results indicate that ATSE can improve the detection rate of 20% on average and filter most false alarms generated by Snort.

The rest of this paper is organized as follows. The related research work is reviewed in Section 2. In Section 3, the basic framework that involves both cyber and physical components is introduced, and a cyber–physical attack case is constructed that can bypass traditional detection mechanism. Details of our proposed ATSE methodology are presented in Section 4. In Section 5, traverse attacks are simulated on three IEEE standard systems to compare the performance of various detection methods. The concluding remarks then follow.

## 2. Related work

Security issues have always been the primary concern since Smart Grid concept was proposed. Smart meter worm was firstly proposed in 2009, which could self-propagate across a large number of intelligence devices in Smart Grid [12]. Various vulnerabilities are explored and collected to develop the security risk evaluation toolbox for Smart Grid devices [13]. Many researchers have investigated how to construct and inject a false data into power system without triggering the bad data detection system based on state estimation [5,14,15]. The US National Institute of Standards and Technology lays out the guidelines for developers and policy makers, covering cyber security requirements of the Smart Grids that should be included from the beginning of the development process [16]. Most countermeasures against Smart Grid attacks are proposed either from the cyber security perspective with the help of information technology, or from the physical side utilizing the physical topology and model.

Some research efforts have been carried out to address the security issues in power system. In 2006, Yu et al. proposed a probabilistic assessment and an integrated risk assessment to assess the cyber vulnerabilities in power industry [17]. Kundur et al. presented a framework to analyze the impact of cyber attacks exerted on Smart Grid [18]. Gharavi and Hu proposed a dynamic key refreshment mechanism to enhance the security of IEEE 802.11s standards against the DoS/DDoS attack in Smart Grid [19]. Kher et al. proposed a model for monitoring the Smart Grid for malicious activities or attacks using machine learning methods [20]. Fouda et al. proposed a lightweight message authentication scheme using Diffie–Hellman exchange protocol in order to achieve mutual authentication and establish the shared session key between the smart meters [21]. In Cisco Smart Grid Framework, security concern plays the role across all functional components [22].

Since Liu et al. found the attackers could inject the false data into power system in 2009 [5], many methods have been proposed to find the bad data. Kim introduced a fast greedy algorithm to select a subset of measurements immune to attacks in order to defend against malicious data injection [23]. Bobba et al. explored the detection of bad data injection attacks through protecting a strategically selected set of sensor measurements [15]. Esmalifalak analyzed the attack risk in electricity market, and modeled the behavior of attack and defender based on game theory [24]. Cui et al. designed a fast detection method based on the adaptive Cumulative Sum (CUSUM) test to defend a subset of critical smart meters [25]. Valezunela exploited Principal Component Analysis (PCA) to separate the power flow variability into regular space and irregular space, which can be further analyzed to identify the existence of compromised measurements in Smart Grid [26]. Liu et al. proposed a bad data detection method based on adaptive partitioning state estimation, which can raise the detection sensitivity by dividing the global power system into several subsystems. Bad data then can be located in a small area by multiple rounds of partition [27].

However, Smart Grid is a typical cyber–physical system, in which the countermeasures simply from the cyber or physical side may be incapable and inadequate [8]. For cyber defense, the properties of electrical parameter have not been considered, which offers little effort in understanding the business of power system. For physical defense, the integrity and validity of power grid data cannot be ensured. Once attack is launched, both cyber network and power grids will present interactive reaction in different forms. Especially, considering the numerous hackers with various motivations, the wide range of attacks with different objectives, the decentralized nature of the control, and the lack of coordination among independent entities, these new security concerns require an advanced security mechanism specialized in the context of Smart Grid.

In recent research, fusion is proposed as a novel cyber–physical solution which can make use of the information obtained from the cyber network as well as the knowledge inherent in the physical system. Zonouz et al. proposed SCPSE, a security-oriented cyber–physical fusion method to identify the bad data injection in Smart Grid [11]. An attack graph template is generated to wipe out the suspected set of measurements in the IDS trigger log for state estimation. Bad data injection is then identified using the Chi-square test, which can largely decrease the computational complexity and improve the detection precision. But the observability of the left measurements and the construction method of attack graph are two big problems for the SCPSE. Sun et al. developed a cyber–physical monitoring system to detect Smart Grid attacks. The network traffic and power measurements were presented in the form of discrete events as abnormal alerts in Snort logs and inconsistent power usage alarms [28]. However, the correlation between the cyber and physical abnormals are not considered.

In this paper, we focus on how to fuse the network traffic and power measurements to improve the attack detection accuracy in Smart Grid, without changing the system topology and introducing extra computation cost.

## 3. Preliminaries and attack case

For the possible attacks in Smart Grid, our proposed method targets the data attacks. It refers to arbitrary attack that modifies the reported power data from the sensor through network intrusion, instead of physically changing the real power flow or topology. As one of the most common and severe attacks in power system, data attacks usually make use of system error tolerance to bypass the traditional bad data detection method, which is hard to be detected. Launching such attacks through cyber network instead of physical access would provide a much easier way for adversary to inject modified data, adding great difficulty to secure data privacy in Smart Grid. Therefore, our framework for correspondent detection mechanism is specially tailored to utilize cross-validation, which involves both the cyber and physical defense strategies. For the cyber network, snort is deployed to monitor the network communication and detect abnormal traffic packets; For the physical system, the widely adopted state estimation in power system is exploited to reduce the observation errors, estimate the electrical states, and detect false data.

### 3.1. Attack detection in cyber network

Snort, a famous light-weight IDS, is adopted to monitor the network traffic, with detection rules designed to support the Modbus protocol (one of most famous light weight protocols in SCADA). Compared with computer networks, the communication protocols used in power system are relatively limited in numbers and forms, and the traffic flow is rather fixed for certain control functions and transmission request. Thus, it is viable for the administrators to summarize the commands with high threat and privilege in the local system. The packet features of these commands are easily extracted for detection in the communication network. The rule-based IDS, such as Snort, is an effective and accuracy solution for Smart Grids.

The snort rules are designed to capture the sensitive or abnormal operations on smart meter that may influence the power grid respond to certain control command and request. All the abnormal packets that are used to read or write the important and sensitive states of the smart meter, such as writing request and operations to certain coils and registors that are used for sensitive and critical parameters, would be alerted as possible system attacks. For example, frequent reading requests to “PASSWORD” state may be used for attackers to crack the password of smart meter; writing requests to the registors for “Primary Current” and “Secondly Current” can be used by the adversary to modify the mutual inductor ratio, which may tamper the smart meter readings for freeloading energy usage.

```
alert tcp $CLIENT_MODBUS_NET any ->
$SERVER_MODBUS_NET 502 (content:"|00 00|"; offset: 2;
depth:2; content: "|10|"; offset: 7; depth: 1; content: "|c3|"; offset:
8; depth: 1; content: "|5b|"; offset: 9; depth: 1; flow: established,
to_server; msg: "Possible MODBUS Parameter Modification
Behavior (primary current)"; sid:1000002; priority:4; )
```

Above is a sample rule designed and exploited to detect the possible modification behaviors of the primary current. Here, alert defines the rule actions that will generate alarms when rule criteria are matched; tcp is the protocol type that is monitored by Snort; $CLIENT_MODBUS_NET any ->$SERVER_MODBUS_NET 502 defines the IP address, port number and direction operator of the traffic flow, setting to match all the client devices talking with smart meter using Modbus communication protocol (502 is the port number for Modbus Protocol). The section enclosed in parenthesis is the rule criteria, matching all the data packets executing writing operations on registor C35B (registor for storing primary current parameter of SIMENSE PAC 4200 Smart Meter).

In our work, several rules are defined with different signatures and threat priorities, including the possible device information modification, possible DOS attack behavior, possible password cracking and possible parameter modification. And three different brands of smart meters including GE, Siemens, and Schneider, are explored for the sensitive registors of critical electric parameters that may become the targets for the malicious attackers, as listed in Table 1. The operations on these registors will be captured as possible attack incidents with the attack type indicating the related electric parameters.

**Table 1**
Sensitive registor and parameter information.

| Meter | Possible attack incidents | | |
|---|---|---|---|
| | Sensitive registor | Parameter information | Sensitive level |
| *GE EPM* 9800 | B354-B355 | Primary current | High |
| | B356-B357 | Secondly current | High |
| | FF23-FF27 | Password | High |
| | 00226-00227 | Active power | Low |
| | 01014-01017 | Total real energy | Low |
| *Siemens PAC*4200 | C35B | Primary current | High |
| | C35D | Secondly current | High |
| | FF0E | Password | High |
| | 11736 | Active power | Low |
| | 11808 | Total real energy | Low |
| *Schneider PM* 800 | 0C81 | Primary current | High |
| | 0C82 | Secondly current | High |
| | 1143 | Active power | Low |
| | 1716 | Real total energy | Low |

**Table 2**
Threat value.

| Target | Operations | |
|---|---|---|
| | Writing | Reading |
| *High sensitive level registor* | IV | III |
| *Low sensitive level registor* | II | I |

Besides, an attack priority will be attached according to the registor number and its sensitive level. Accordingly, a threat value will also be assigned as the priority knowledge to evaluate the possible influence posted by certain attack behavior. For example, it might be the data acquisition when we detect several packets which are applied to read the registor of "Meter Name" or "Power Consumption". But the writing operation for the "Password" registor would be a serious intrusion. For different systems and various devices, this binding threat value is only related with the operations on the certain registor, as shown in following Table 2. The correspondent alarms will then be generated and recorded according to Table 2, in the form of an alarm log with tracking clues such as attack type and priority.

At the same time, the features of published attacks would be extracted as the rules added into the IDS. They would be assigned with high treat priority, since they represent a real attack that is launched in the system.

### 3.2. Bad data detection in physical system

State estimation is widely adopted in the power system to provide secure and reliable power delivery. The concept is first introduced into power grid by Schweppe and its primary function is to serve as filters against incorrect power measurements received through the SCADA system [29]. The state variables are related to the measurements:

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e} \tag{1}$$

where $\mathbf{z} = [z_1, z_2, \ldots, z_m]^T$ is the meter measurements and $\mathbf{x} = [x_1, x_2, \ldots, x_n]^T$ stands for the state variables. **h(x)** is the computed estimation results, and $\mathbf{e} = [e_1, e_2, \ldots, e_m]^T$ is the measurement noise which is assumed to follow Gaussian distribution of zero mean. This assumption is generally accepted in power system state estimation formulation. $\mathbf{h}(\mathbf{x})$ can be further rewritten as follows:

$$\mathbf{h}(\mathbf{x}) = [h_1(x_1, x_2, \ldots, x_n), \ldots, h_m(x_1, x_2, \ldots, x_n)]^T \tag{2}$$

where $h_l(x_1, x_2, \ldots, x_n)$ is a function of $x_1, x_2, \ldots, x_n$. Note that in power state estimation, real-time redundant measurements, such as the branch active power, branch reactive power, bus active power injection and bus reactive power injection, are applied to estimate the unknown states, including the bus voltage magnitude and voltage phase, based on the system topology and physical constrains, which help to improve data accuracy and automatically excluded from the error message caused by random interference. Essentially the estimation requires the amount of measurements to outnumber the state variables.

Essentially, power system state estimation is a process which uses real-time redundant measurements to improve data accuracy and automatically is excluded from the error message caused by random interference. The objective is to find an estimate $\hat{\mathbf{x}}$ of $\mathbf{x}$ that is the best fit of the measurement $\mathbf{z}$ according to (1). The problem is usually solved by the Weighted Least Squares (WLS) Algorithm. The state estimation can be formulated as a quadratic optimization problem:

$$\min_{\mathbf{x}} J(\mathbf{x}) = \min_{\mathbf{x}} [\mathbf{z} - \mathbf{h}(\mathbf{x})]^T \mathbf{R}^{-1} [\mathbf{z} - \mathbf{h}(\mathbf{x})] \tag{3}$$

where $\mathbf{R}^{-1}$ is the measurement inverse covariance matrix. Newtown's method can be applied to solve the quadratic optimization problem. The increment can be calculated by

$$\Delta x^{(k)} = G(x^{(k)})^{-1} H^T(x^{(k)}) \cdot R^{-1} \cdot [z - h(x^{(k)})] \tag{4}$$

where $H(x^{(k)}) = \left.\frac{\partial h(x)}{\partial (x)}\right|_{x=x^{(k)}}$ is the Jacobi matrix and $G(x^{(k)}) = H^T(x^{(k)}) R^{-1} H(x^{(k)})$ is the gain matrix. The convergence criterion is the following:

$$\max\left(\left|\Delta x^k\right|\right) < \varepsilon_x \tag{5}$$

where $\varepsilon_x$ is a predefined threshold.

The measurements might be inaccurate because of device misconfiguration, device failures, malicious actions or other errors. Chi-square test is a common approach for detecting bad data according to the measurement residuals:

$$J(\hat{\mathbf{x}}) = \sum_{i=1}^{m} \frac{(z_i - h_i(\hat{\mathbf{x}}))^2}{\sigma_i^2}. \tag{6}$$

Assuming that all state variables are mutually independent and the sensor errors follow a normal distribution, the measurement residuals $J(\hat{\mathbf{x}})$ follow a chi-squared distribution $\chi^2_{(m-n)}$ with $m - n$ degrees of freedom.

The steps of the Chi-square test are given as follows:

(1) Solve the WLS estimation problem and compute the measurement residuals $J(\hat{\mathbf{x}})$.
(2) The threshold $\chi^2_{(m-n),p}$ is determined through a hypothesis test with a significance level $p$ (*e.g. 95%*).
(3) If $J(\hat{\mathbf{x}}) \geq \chi^2_{(m-n),p}$, then bad data will be suspected. Otherwise, the measurements will be assumed to be free of bad data.

### 3.3. Attack case against IEEE 14-bus system

An attack case is constructed to inject bad data on IEEE 14-bus system, as shown in Fig. 1. The original measurements are simulated by MATPOWER and the Gaussian noise is then added.

As shown in Table 3, the measurements on the transmission lines between bus 1 and 2 ($L_{1,2}$) are revised. The power flow from bus 1 to bus 2, observed on bus 1 ($P_{1,2}$) is modified from 156.88 to 203.95 MW; the $P_{2,1}$ is modified from −152.59 to −198.36 MW to keep the conservation of energy. (Generally, the $P_{i,j}$ is not equal to $P_{j,i}$, because of the line losses.) The Chi-square test is applied to detect the bad date from all measurements. In our work, Chi-square test is solved by MATPOWER. The weighted sum-squared residual $J(\hat{\mathbf{x}})$ is 50.66, which is lower than the threshold of IEEE 14-bus system 72.15. Thus, the bad data could not be detected using the traditional state estimation and bad data detection method. And the high false negative rate may cause potential energy theft or even some more serious harms, such as the false control command to cut off the transmission lines.

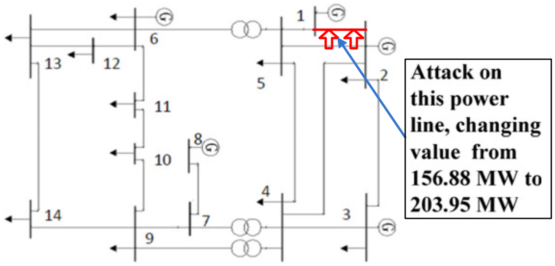

1
2
3
4
5
6
7
8
9
10
11
12
13
14
Attack on this power line, changing value from 156.88 MW to 203.95 MW

**Fig. 1.** Attack Case on IEEE 14-bus system.

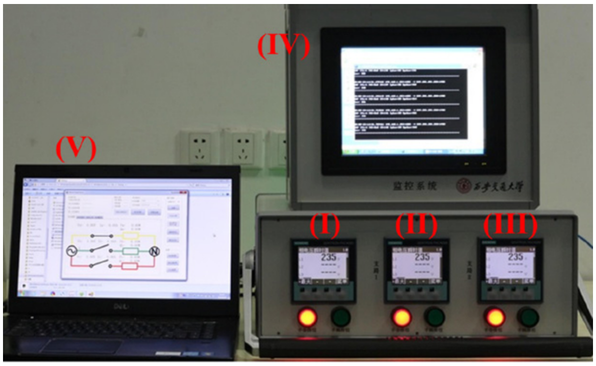


**Fig. 2.** A micro grid experiment testbed.

**Table 3**
Injected data of the attack case.

| Bus | | Power flow (MW) | | Detection | |
|---|---|---|---|---|---|
| From | To | Original | Injected | Threshold | $J(\hat{\mathbf{x}})$ |
| 1 | 2 | 156.88 | 203.95 | 72.15 | 50.66 |
| 2 | 1 | −152.59 | −198.36 | | |

### 3.4. Attack case in Smart Grid testbed

For the cyber network, the intrusion behavior of the adversary can be captured by Snort through monitoring the network communication traffic. As shown in Fig. 2, a micro grid is set up in our lab. Three SIEMENS PAC 4200 smart meters (I–III) are deployed to measure the circuits, which are connected into the lab network. Their IP address is 192.168.1.2–192.168.1.4. A laptop (V) is an attacker which tries to crack and modify the password (IP is 192.168.1.124). The Snort and data center are installed on a YanHua Industry control machine (IV) to monitor all traffic of lab network and read the data from all meters.

As illustrated in Table 4, IDS technique suffers from the high false positive rate of its alarms. For the twelve alerts generated by Snort, only two of them are real alerts representative of modifications on the password and parameters. However, the other ten records are false alarms which may uncover the real attack incidents launched. The high false positive ratio of cyber alerts makes it difficult to utilize the result of cyber alerts directly. In other words, the Snort abnormal traffic analysis only cannot be the convinced evidence to identify and locate this launched attack. The consistency of the physical data should be exploited to identify and locate the real attacks.

## 4. Abnormal traffic-indexed state estimation

In the above attack case, the adversary can elaborately construct an attack vector that can bypass the traditional detection mechanism, due to the threshold set to tolerate the unpredictable and inevitable errors for state estimation in physical system. Thus, it is difficult to detect the injected data hidden in the normal observation error. If the impact of the possibly modified measurements can be reasonably reduced, the estimation will be more accurate and the detection will be more sensitive.

**Table 4**
Cyber alarms of the attack case.

| IP_src | IP_dst | Sig_name | Priority |
|---|---|---|---|
| 192.168.1.101 | 192.168.1.103 | ICMP PING Windows | 1 |
| 192.168.1.103 | 192.168.1.101 | ICMP Echo Reply | 1 |
| **192.168.1.124** | **192.168.1.103** | **Password modification** | **3** |
| **192.168.1.124** | **192.168.1.103** | **Parameter modification** | **4** |
| 192.168.1.101 | 192.168.1.103 | ICMP PING | 1 |
| 192.168.1.101 | 192.168.1.103 | ICMP L3retriever Ping | 1 |
| 192.168.1.101 | 192.168.1.103 | ICMP PING | 1 |
| 192.168.1.101 | 192.168.1.103 | ICMP PING Windows | 1 |
| 192.168.1.103 | 192.168.1.101 | ICMP Echo Reply | 1 |
| 192.168.1.101 | 192.168.1.103 | ICMP PING | 1 |
| 192.168.1.101 | 192.168.1.103 | ICMP PING NMAP | 1 |
| 192.168.1.103 | 192.168.1.101 | ICMP Echo Reply | 1 |

In ATSE, the abnormal traffic in the cyber system is quantified to serve as one of the impact factors in the physical model. Chi-square test is then used to detect whether bad data exists in the system. The incorporation of the cyber influence into the state estimation model helps to achieve more specific inferences, which may contribute to more accurate detections. The main procedure of ATSE method consists of following steps:

(1) Quantification of the cyber impact;
(2) Integration into the state estimation model;
(3) Bad data detection.

### 4.1. Quantification of the cyber impact

The quantification of the cyber impact should follow several basic rules: (1) the attack incidents with a high threat level should pose a much greater influence than that with a low level. (2) The number of alarms is another factor for impact evaluation. Some attacks, such as device scanning, would cause lots of Modbus connection packets and lower threat alarms. (3) The requirements should be harder as the impact increases. Thus, the accumulations of the cyber impacts should be in a nonlinear manner.

Based on the guidelines above, let $\mathbf{\Omega}$ denote the network impact factor matrix of every bus in the power grid. It can then be determined according to the cyber alert log. The correspondent snort alarms are recorded in an alert log with trace clues, e.g. IP address, attack type and threat priority, as "IP_src | IP_dst | Time | Sig_name | Sig_priority". According to the records of device-IP map, all alert logs of the device $i$ are clustered to calculate the impact factor $\Omega_{im}$:

$$\Omega_{im} = \sum_{k\in alert(device\_i)} m^{priority(k)} \tag{7}$$

where $m$ is the weight coefficient threat priority ($m > 1$), $alert(device\_i)$ is the set of the alerts on device $i$, the $priority(k)$ is the threat priority of the alert $k$. The square root function is then applied to smooth the fast expended increments caused by the cumulative effect, as expressed below:

$$\Omega_i = \sqrt{1 + \sum_{k\in alert(device\_i)} m^{priority(k)}}. \tag{8}$$

A plus of one for $\Omega_{im}$ can guarantee that the quantification increases nonlinearly. The impact factor of all devices are then clustered to form the impact factor matrix $\mathbf{\Omega}$ to quantify the influence of the cyber anomaly on the power grid, which can be expressed as:

$$\mathbf{\Omega} = DiagonalMatrix\left(\Omega_1, \Omega_2, \ldots, \Omega_n\right). \tag{9}$$

### 4.2. Integration into state estimation model

The cyber impact factor matrix $\mathbf{\Omega}$ is merged into the state estimation as a reasonable adjustment of the weight values, thus the objective function $J(\mathbf{x})$ can be modified as:

$$\min_{\mathbf{x}} J_{ATSE}(\mathbf{x}) = \min_{\mathbf{x}} [\mathbf{z} - \mathbf{h}(\mathbf{x})]^T (\mathbf{\Omega R})^{-1} [\mathbf{z} - \mathbf{h}(\mathbf{x})] \tag{10}$$

The WLS algorithm is employed and Newton's method is applied to solve the quadratic optimization problem. The increment can be calculated by

$$\Delta x^{(k)} = G(x^{(k)})^{-1} H^T(x^{(k)}) \cdot (\mathbf{\Omega} R)^{-1} \cdot [z - h(x^{(k)})] \tag{11}$$

which is same as (4), and the convergence criterion is same as (5). According to (10), adding the cyber impact factor can help to derive a much more accurate estimation of the state $x$, marked as $\hat{\mathbf{x}}_{ATSE}$, since influence of the possible malicious modified data can be reduced. Thus, the modeling of the network traffic flow provides a flexible adjustment of the weight assigned to the physical measurements, without changing the original system topology and system observability.

### 4.3. Bad data detection

Chi-square test is used to detect the bad data, which is same as the traditional state estimation. For a well-proofreading system, the measurement noise $e$ is assumed to be a distributed random variable with zero mean and $R$ variance. Thus, the objective function for injected data detection can be rewritten in terms of the measurement error in such a way that:

$$J(\hat{\mathbf{x}}_{ATSE}) = \sum_{i=1}^{m} R_{ii}^{-1}(z - h(\hat{\mathbf{x}}_{ATSE}))^2 = \sum_{i=1}^{m} \left( \frac{e_i}{\sqrt{R_{ii}}} \right)^2 \tag{12}$$

where $e_i$ is the $i$th measurement error, $R_{ii}$ is the diagonal entry of the measurement error covariance matrix and $m$ is the total number of measurements. The objective function will follow a Chi-square distribution with $(m - n)$ degrees of freedom, since $e^i/\sqrt{R_{ii}}$ is a Standard Normal distribution and $n$ measurements satisfy the power balance equations in the power system, which means $(m - n)$ of the measurement errors will be linearly independent. Then, the Chi-square test can be applied as:

$$\begin{cases} J(\hat{\mathbf{x}}_{ATSE}) \geq \chi^2_{(m-n),p} & yes \\ J(\hat{\mathbf{x}}_{ATSE}) < \chi^2_{(m-n),p} & no. \end{cases} \tag{13}$$

With the improved state estimation, the bad data in the power system can be detected and located, which cannot be detected using traditional state estimation method.

## 5. Experiment and analysis

In this section, the performance of ATSE is evaluated. In Section 5.1, the previous attack case on IEEE 14-bus system is used to verify the effectiveness of our proposed ATSE method. In Section 5.2, large number of experiments are carried out including 80 normal cases with different cyber false alarm scenarios and a traverse attack case on the IEEE-14 bus system, to evaluate the performance of ATSE, and present a statistical comparison of detection performances between the traditional state estimation and ATSE methods.

### 5.1. Case study on IEEE-14 bus system

The elaborate constructed attack vector that can bypass the traditional detection methods in the previous attack case is selected to evaluate the performance of our proposed solution. Using ATSE, the cyber impact factor is first calculated according to (4).

**Table 5**
Cyber impact factor of the attack case.

| Cyber alert | Attack type | Threat priority | Weight coefficient | Cyber impact |
|---|---|---|---|---|
| $L_{1,2}$ | Parameter writing | IV | 16.0 | 4.06 |
| | Password writing | II | 1.5 | |
| $L_{2,3}$ | Parameter reading | III | 2.89 | 2.26 |
| | Password reading | I | 1.1 | |
| | Device info reading | I | 1.1 | |
| $L_{4,7}$ | Parameter reading | III | 2.89 | 1.99 |
| | Device info reading | I | 1.1 | |
| $L_{5,6}$ | Device info reading | I | 1.1 | 1.05 |
| $L_{6,11}$ | Parameter reading | II | 1.5 | 1.61 |
| | Device info reading | I | 1.1 | |
| $L_{12,13}$ | Parameter reading | I | 1.1 | 1.48 |
| | Device info reading | I | 1.1 | |

**Table 6**
Estimation result comparison.

| Line # | Modified measurement | | Estimated measurement | |
|---|---|---|---|---|
| | Original Value | Injected Value | ATSE | Traditional SE |
| $Line_{1,2}$ | 156.88 | 203.95 | 175.11 | 204.53 |
| $Line_{1,5}$ | 75.51 | 75.51 | 80.97 | 83.92 |
| $Line_{2,3}$ | 73.24 | 73.24 | 72.12 | 72.89 |
| $Line_{2,4}$ | 56.13 | 56.13 | 57.24 | 49.33 |
| $Line_{2,5}$ | 41.52 | 41.52 | 42.15 | 35.98 |
| $Line_{4,7}$ | 28.07 | 28.07 | 26.08 | 27.80 |
| $Line_{5,6}$ | 44.09 | 44.09 | 45.14 | 41.82 |
| $Line_{6,11}$ | 7.35 | 7.35 | 7.43 | 6.98 |
| $Line_{12,13}$ | 1.61 | 1.61 | 4.01 | 0.56 |

As listed in Table 5, the cyber impact is then added into the estimation model, and the results derived are shown in following Table 6.

Chi-square test is then applied to detect bad data. The value of $J(\hat{\mathbf{x}}_{ATSE})$ is 233.29 which greatly exceeds the threshold $T_{o,p} = 72.15$ and implies bad data existed in the system. $J(\hat{\mathbf{x}})$ using traditional state estimation is below the threshold, which is 50.66 computed in Section 3. It is demonstrated in this case that ATSE can identify the injected malicious data that is undetectable by the traditional method. And the reason is ATSE could result in a more precise estimation. Detailed analysis and comparison of the estimation process between ATSE and traditional method are also listed in Table 6. The estimated measurement of line $L_{1,2}$ using traditional state estimation is 204.53 MW, which is close to the injected data (203.95 MW); while the estimated value of line $L_{1,2}$ using ATSE is 175.11 MW, which is a much more specific inference to the real data (156.88 MW). Obviously, the ATSE can greatly reduce the influence of the modified measurements. Besides, considering the possible influence on the neighboring buses, its adjacent lines $L_{1,5}$, $L_{2,4}$, $L_{2,5}$ are also compared. And the estimated results using traditional method are 83.92 MW, 49.33 MW and 35.98 MW, respectively; while the estimation result using ATSE is 80.97 MW, 57.24 MW and 42.15 MW, respectively. These supposed influenced lines are still of the same trend that tends to converge to the real measurements compared with traditional method. Therefore, it is obvious that our proposed ATSE can achieve a much more precise estimation inference on the injected power line due to the integration of the cyber impact of the modification behavior captured by Snort, even with the high false alarms.

Besides, the traverse attack is conducted on IEEE 14-bus system, consisting of 14 buses and 20 transmission lines, to compare the detection precision of ATSE and traditional state estimation method. For each of the transmission lines, we modify the measurement of the active power on this line by multiplying 1.3 to the

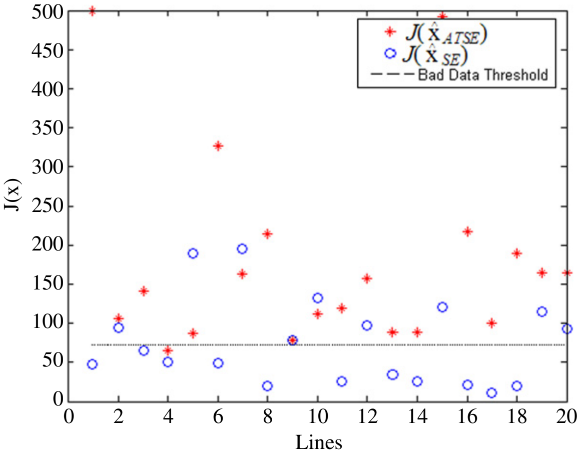


**Fig. 3.** Detection results.

real measurement and then record the total number of successful detections after traversing all these power lines. For each attack, 2 real alarms are generated to log the event of data modification on both sides of the target transmission line; while 10 false alarms are generated randomly. Since the data on all buses should follow power balance, the attackers have to modify the data on transmission line, load and generator simultaneously. In this paper, we only discuss the transmission line BDI; and the load/generator BDI could be detected using the same method.

The detection precisions of ATSE and traditional method are illustrated in Fig. 3. In all 20 attacks, traditional state estimation can only detect 9 of the injected data with only 45% detection precision while our proposed ATSE can detect 19 of all the attacks, which greatly improve the detection precision to 95%. This indicates that ATSE is capable of acquiring more accurate detection for bad data injection attacks in Smart Grid.

### 5.2. Cyber false alarm influence analysis

In this section, the possible influence of the false cyber alarms on our proposed ATSE method is further investigated on IEEE-39 bus system, consisting of 39 buses and 46 transmission lines. The false alarm rate can be defined as :

$$FAR = \frac{N_{sa} - N_{ra}}{N_{sa}} * 100\% \tag{14}$$

where $N_{sa}$ is the total cyber alarms captured by Snort; $N_{ra}$ is the number of real alarms that existed in the system. Different levels of *FAR* are set to compare the detection rate of ATSE and traditional state estimation method using a traverse attack on all the 46 transmission lines.

For each of the transmission lines, the measurement of the active power is multiplied by 1.3 to the real measurement and then 100 experiments with random false alarms generated at different *FAR* levels are conducted. The total number of successful detection using ATSE and Traditional State Estimation is recorded as the detection rate in Table 7. ATSE has a persistent better performance than the traditional method. ATSE can detect 45 of 46 attacks at $FAR = 90\%$, 44 of 46 attacks at $FAR = 97\%$ and $FAR = 99\%$, respectively in the optimal condition. By contrast, traditional state estimation can only detect 34 of 46 attacks even in the optimal case. Injection on $L_{1,39}$, $L_{2,30}$, $L_{3,4}$, $L_{3,18}$, $L_{8,9}$, $L_{9,39}$, $L_{12,13}$, $L_{14,15}$, $L_{16,24}$, $L_{17,27}$, $L_{19,20}$ and $L_{22,23}$, which cannot be detected using the traditional method, can be partially detected by ATSE except for $L_{12,13}$. The reason for not being fully detected is that the original measurements on these power lines are at least five times smaller than the rest of the measurements, which indicates that 30% injection can still be covered by the observation noise even with an amendment using relevant measurements of neighboring buses. However, considering the attacker's effort and benefits of launching attacks, those power lines with larger measurements would be malicious modified with a higher possibility.

**Table 7**
Detection rate with different FARs.

| Line # | ATSE | | | Traditional SE |
|---|---|---|---|---|
| | $FAR = 90\%$ | $FAR = 97\%$ | $FAR = 99\%$ | |
| $Line_{1,2}$ | 100% | 100% | 100% | 100% |
| $Line_{1,39}$ | 77% | 82% | 71% | 0% |
| $Line_{2,3}$ | 100% | 100% | 100% | 100% |
| $Line_{2,25}$ | 100% | 100% | 100% | 63% |
| $Line_{2,30}$ | 65% | 57% | 61% | 0% |
| $Line_{3,4}$ | 18% | 13% | 15% | 0% |
| $Line_{3,18}$ | 30% | 28% | 27% | 0% |
| $Line_{4,5}$ | 100% | 100% | 100% | 100% |
| $Line_{4,14}$ | 100% | 100% | 100% | 100% |
| $Line_{5,6}$ | 100% | 100% | 100% | 100% |
| $Line_{5,8}$ | 100% | 100% | 100% | 100% |
| $Line_{6,7}$ | 100% | 100% | 100% | 100% |
| $Line_{6,11}$ | 100% | 100% | 100% | 100% |
| $Line_{6,31}$ | 100% | 100% | 100% | 100% |
| $Line_{7,8}$ | 100% | 100% | 100% | 100% |
| $Line_{8,9}$ | 20% | 14% | 14% | 0% |
| $Line_{9,39}$ | 25% | 24% | 20% | 0% |
| $Line_{10,11}$ | 100% | 100% | 100% | 100% |
| $Line_{10,13}$ | 100% | 100% | 100% | 100% |
| $Line_{10,32}$ | 100% | 100% | 100% | 100% |
| $Line_{12,11}$ | 100% | 100% | 100% | 100% |
| $Line_{12,13}$ | 1% | 0% | 0% | 0% |
| $Line_{13,14}$ | 100% | 100% | 100% | 100% |
| $Line_{14,15}$ | 35% | 33% | 30% | 0% |
| $Line_{15,16}$ | 100% | 100% | 100% | 95% |
| $Line_{16,17}$ | 100% | 100% | 100% | 21% |
| $Line_{16,19}$ | 100% | 100% | 100% | 2% |
| $Line_{16,21}$ | 100% | 100% | 100% | 100% |
| $Line_{16,24}$ | 33% | 27% | 26% | 0% |
| $Line_{17,18}$ | 100% | 100% | 100% | 20% |
| $Line_{17,27}$ | 15% | 12% | 10% | 0% |
| $Line_{19,20}$ | 58% | 53% | 43% | 0% |
| $Line_{19,33}$ | 100% | 100% | 100% | 46% |
| $Line_{20,34}$ | 100% | 100% | 100% | 7% |
| $Line_{21,22}$ | 100% | 100% | 100% | 100% |
| $Line_{22,23}$ | 31% | 29% | 28% | 0% |
| $Line_{22,35}$ | 100% | 100% | 100% | 29% |
| $Line_{23,24}$ | 100% | 100% | 100% | 100% |
| $Line_{23,36}$ | 100% | 100% | 100% | 100% |
| $Line_{25,26}$ | 84% | 81% | 77% | 7% |
| $Line_{25,37}$ | 100% | 100% | 100% | 89% |
| $Line_{26,27}$ | 100% | 100% | 100% | 100% |
| $Line_{26,28}$ | 100% | 100% | 100% | 100% |
| $Line_{26,29}$ | 100% | 100% | 100% | 100% |
| $Line_{28,29}$ | 100% | 100% | 100% | 100% |
| $Line_{29,38}$ | 100% | 100% | 100% | 100% |

Besides, from Table 7, a general trend of slight decrease of ATSE detection rate is reflected with higher false alarm rate, though it is still more accurate compared with the traditional state estimation method. This can be illustrated as higher *FAR* will reduce the correction capacity of the related neighboring measurements, therefore leading to uncover some real attack behaviors. However, compared with the false alarm rate of the cyber network, ATSE has greatly reduced the false positive rate. Details are analyzed as follows.

Another 3 groups of experiments are carried out with no attack. In each group, 4600 normal cases are conducted at different false alarm rates $FAR = 90\%$, $FAR = 97\%$ and $FAR = 99\%$ to analyze the false positive rate (FPR) and false negative rate (FNR) of ATSE, as listed in Table 8. None normal cases are identified as attack both in the ATSE and Chi-square test. Thus, the FPR is 0 in all experiments. While, the FNR of ATSE is dramatically lower than the Chi-square test about 20%.

**Table 8**
False positive/negative rate.

| Experiments | | FPR | FNR |
|---|---|---|---|
| ATSE | *FAR* = 90% | 0% | 17.57% |
| | *FAR* = 97% | 0% | 18.41% |
| | *FAR* = 99% | 0% | 19.08% |
| | Traditional SE | 0% | 39.59% |

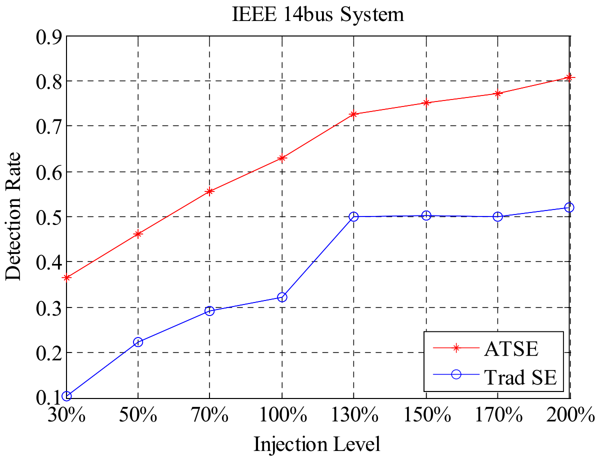


**Fig. 4.** Detection rate on IEEE-14 bus system.

### 5.3. Cyber alarm injection capacity analysis

The impact that different cyber alarm injection capacities impose on the performance of our proposed ATSE is analyzed in this section. The capacity of the cyber alarm is defined as the injection level *INL* to assess the relative injected errors against the original measurement values:

$$INL = \left|\frac{P_{inj} - P_{org}}{P_{org}}\right| * 100\% \tag{15}$$

where $P_{org}$ is the original measurement and $P_{inj}$ is the injected data. Nine groups of traverse attack with different *INLs* are launched on IEEE-14, 39 and 118 bus system to compare the detection rate of ATSE and the traditional state estimation method. For each group of the traverse attack, 100 experiments with random cyber alarms will be generated on each bus. The FAR of cyber alarm is set as 97% in the session.

For IEEE 14-bus system, 8 different *INLs* are set from 30% to 200%. With each *INL*, 100 attack cases are simulated to inject bad data into each of 20 transmission lines. The detection is calculated as the total number of identified attacks in all of the 2000 cases. As shown in Fig. 4, ATSE can detect 733 of 2000 (37%) attacks when *INL* is 30%, which is 20% higher than the traditional method that can detect only 210 of 2000 (10.5%) attacks. With the increment of the *INL*, the detection rate increases persistently. When the injection level reaches 200%, the detection rate of ATSE is over 80%, which is much higher compared with the traditional method that can only detect 1040 of 2000 (52%) attacks.

For IEEE 39-bus system, 8 different *INLs* are set from 30% to 200%. Totally 4600 experiments are carried out with 100 cases on 46 transmission lines. As shown in Fig. 5, ATSE can detect 3789 of 4600 attacks (the detection rate is 82.37%) at injection level *INL* = 30%. While the detection rate of Chi-square test is 60.41%, which indicates ATSE still performs much better than traditional methods. When the *INL* is higher than 100%, ATSE can detect more 95% attacks, which outperforms the traditional method.

In IEEE 118-bus, there are 186 transmission lines and 744 measurements. Compared with 14-bus (20 lines and 80 measurements) and 39-bus (46 lines and 184 measurements), the system size of 118-bus is several times larger. It would result in a higher tolerance for observation errors and measurement noises. Accordingly, the *INLs* should be adjusted to deal with the changes in system error-tolerance, which are set from 100% to 400%. As shown in Fig. 6, when *INL* is 100%, over 38% of attacks can be detected using ATSE, yet only 25% attacks can be detected using traditional state estimations. This difference will be enlarging with the increasing of *INL*. ATSE can detect 82.7% attacks when INL is 400%, while the traditional method can detect only 58.4% of all the attacks at the same *INL*.

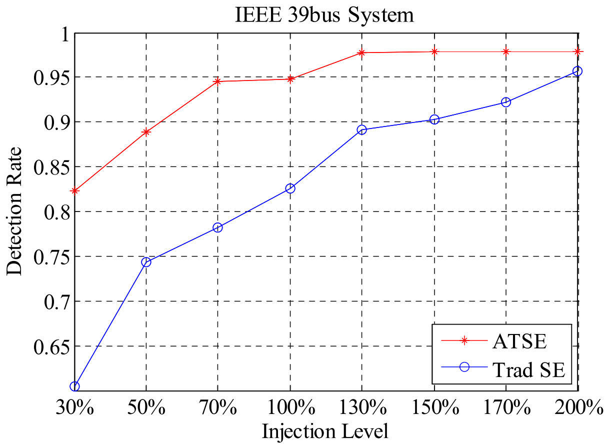


**Fig. 5.** Detection rate on IEEE 39-bus system.

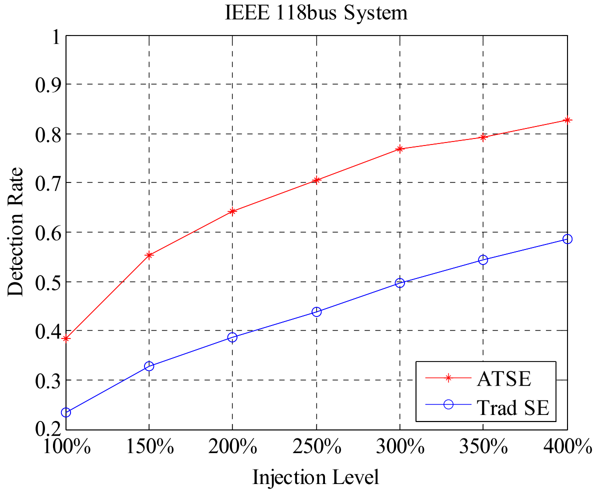


**Fig. 6.** Detection rate on IEEE 118-bus system.

For IEEE 14, 39 and 118 bus systems, the detection rate of ATSE is 20% higher than traditional methods on average. Thus, it is proved that ASTE has a persistent better performance than the traditional state estimation method from the tremendous experiments carried out with different *INL* levels on different IEEE standard bus systems.

### 5.4. Observability discussion

Observability is a measure for how well internal states of a system can be inferred by the outputs. For state estimation, a system is said to be observable if the current state can be determined in finite time using the measurements. In current power system, the engineers have designed the meter deployment plan to make sure the there are enough measurements to estimate all states of the whole system.

In SCPSE [11], the suspected measurements would be removed and the system function **h(x)** in Eq. (1) would be changed. The left system would not be observable. In the experiments, three groups of simulations are conducted on IEEE 39-bus system. In group A, 46 transmission lines are removed one by one in 46 simulation cases; in group B, 100 cases are simulated, in which 3 transmission lines are randomly selected and removed; in group C, 4 transmission lines are randomly removed in each case. It is shown that 11 cases in group A (24%) are unobservable and fail to solve using state estimation; only 65 cases in group B (65%) are unobservable; no case in group C is observable.

Considering the high false positive of IDS, the observability would be a great problem for SCPSE. As shown in group C, when 8.7% transmission lines are identified as suspected, the state estimation and bad data detection system would be broken down.

In ATSE, the weight of suspected data is decreased. Thus, the observability and state estimation process would not be changed and all cases could be solved successfully. As shown in Section 5.3, even if the FAR is as high as 99%, ATSE could detect BDI attacks with a high precision.

## 6. Conclusion

In this paper, a cyber–physical fusion method is proposed to detect the bad data injection attack in Smart Grid. Extensive experiments in IEEE 14, 39 and 118 bus systems prove that combining the cyber impact in conjunction with the inherent physical topology and restriction is capable of identifying the hybrid attacks and locating certain undetected attacks that are insensitive to the traditional state estimation method.

The basic idea of ATSE is that the discrete event is quantified as the index of physical system model. It demonstrates a low-cost and easy-implement solution to integrate heterogeneous data in Smart Grids, since the cyber monitoring methods and physical models are deployed in the current Internet and power system. Moreover, ATSE could be extended to detect other attacks in various cyber–physical systems.

For future work, the correlation and interaction between the cyber network and power system will be further investigated. The topology of Smart Grids will be added into the cyber impact quantification. More IDS tools and abnormal detection methods in computer network will be explored and integrated into ATSE. Moreover, how to evaluate the cyber impact in the various Smart Grids will be studied.

## Acknowledgments

The research presented in this paper is supported in part by the National Natural Science Foundation of China (91118005, 91218301, 61221063, 61203174, 61472318, U1301254), 863 High Tech Development Plan (2012AA011003) and Key Project of the National Research Program of China (2012BAH16F02).

## References

[1] H. Khurana, M. Hadley, N. Lu, D.A. Frincke, Smart-grid security issues, IEEE Secur. Priv. 8 (2010) 81–85. 2010-01-01.

[2] W. Wang, Z. Lu, Cyber security in the smart grid: Survey and challenges, Comput. Netw. 57 (2013) 1344–1371.

[3] P. McDaniel, S. McLaughlin, Security and privacy challenges in the smart grid, IEEE Secur. Priv. 7 (2009) 75–77.

[4] L. Xie, Y. Mo, B. Sinopoli, False data injection attacks in electricity markets, in: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, 2010, pp. 226–231.

[5] Y. Liu, P. Ning, M.K. Reiter, False data injection attacks against state estimation in electric power grids, TISSEC 14 (2011) 13.

[6] D. Wang, X. Guan, T. Liu, Y. Gu, C. Shen, Z. Xu, EDSE: A Detection Method Against Tolerable False Data Injection Attack in Smart Grid, Energies 7 (2014) 1517–1538.

[7] T.M. Chen, Stuxnet, the real start of cyber warfare? [Editor's Note], IEEE Netw. 24 (2010) 2–3.

[8] Y. Mo, T. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, B. Sinopoli, Cyber-physical security of a smart grid infrastructure, Proc. IEEE 100 (2012) 195–209.

[9] Y. Gu, T. Liu, D. Wang, X. Guan, Z. Xu, Bad data detection method for smart grids based on distributed state estimation, in: Communications (ICC), 2013 IEEE International Conference on, 2013, pp. 4483–4487.

[10] O. Kosut, L. Jia, R.J. Thomas, L. Tong, Malicious data attacks on the smart grid, in: Smart Grid, IEEE Transactions on, vol. 2, pp. 645–658, 2011.

[11] S. Zonouz, K.M. Rogers, R. Berthier, R.B. Bobba, W.H. Sanders, T.J. Overbye, SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures, in: Smart Grid, IEEE Transactions on, vol. 3, pp. 1790–1799, 2012-01-01, 2012.

[12] M. Davis, SmartGrid Device Security: Adventures in a New Medium, in: *Black Hat*, Las Vegas, USA, 2009.

[13] Y. Liu, J. Liu, T. Liu, X. Guan, Y. Sun, Security risks evaluation toolbox for smart grid devices, in: Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM, 2013, pp. 479–480.

[14] O. Kosut, L. Jia, R.J. Thomas, L. Tong, Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures, in: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, 2010, pp. 220–225.

[15] R.B. Bobba, K.M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, T.J. Overbye, Detecting false data injection attacks on dc state estimation, in: Preprints of the First Workshop on Secure Control Systems, CPSWEEK, 2010.

[16] Office of the national coordination for smart grid interoperability, in: NIST framework and roadmap for smart grid interoperability standards. http://www.nist.gov.

[17] J. Yu, A. Mao, Z. Guo, Vulnerability assessment of cyber security in power industry, in: in Power Systems Conference and Exposition, 2006. PSCE'06. 2006 IEEE PES, 2006, pp. 2200–2205.

[18] D. Kundur, X. Feng, S. Liu, T. Zourntos, K.L. Butler-Purry, Towards a framework for cyber attack impact analysis of the electric smart grid, in: Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, 2010, pp. 244–249.

[19] H. Gharavi, B. Hu, Dynamic key refreshment for smart grid mesh network security, in: Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES, 2013, pp. 1–6.

[20] S. Kher, V. Nutt, D. Dasgupta, H. Ali, P. Mixon, A detection model for anomalies in smart grid with sensor network, in: Future of Instrumentation International Workshop (FIIW), 2012, pp. 1–4.

[21] M.M. Fouda, Z.M. Fadlullah, N. Kato, R. Lu, X. Shen, Towards a light-weight message authentication mechanism tailored for smart grid communications, in: Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on, 2011, pp. 1018–1023.

[22] Cisco. Security for the Smart Grid. 2009. http://www.cisco.com/web/strategy/docs/energy/white_paper_c11_539161.pdf.

[23] T.T. Kim, H.V. Poor, Strategic protection against data injection attacks on power grids, in: Smart Grid, IEEE Transactions on, vol. 2, pp. 326–333, 2011.

[24] M. Esmalifalak, G. Shi, Z. Han, L. Song, Bad data injection attack and defense in electricity market using game theory study, 2013.

[25] S. Cui, Z. Han, S. Kar, T.T. Kim, H.V. Poor, A. Tajer, Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions, in: Signal Processing Magazine, IEEE, vol. 29, pp. 106–115, 2012.

[26] J. Valenzuela, J. Wang, N. Bissinger, Real-time intrusion detection in power system operations, in: Power Systems, IEEE Transactions on, vol. 28, 2013, pp. 1052–1062.

[27] T. Liu, Y. Gu, D. Wang, Y. Gui, X. Guan, A novel method to detect bad data injection attack in smart grid, in: INFOCOM, 2013 Proceedings IEEE, 2013, pp. 3423–3428.

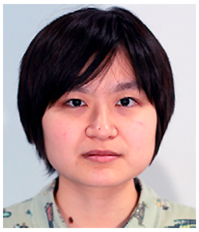
[28] Y. Sun, X. Guan, T. Liu, Y. Liu, A Cyber-Physical Monitoring System for Attack Detection in Smart Grid, in: IEEE INFOCOM 2013 Demo/Poster Session, pp. 1416–1417, 2013.

[29] F.C. Schweppe, D.B. Rom, Power system static-state estimation, Part II: Approximate Model, Power Apparatus and Systems, IEEE Transactions on, pp. 125–130, 1970.

**Ting Liu** received his B.S. degree in Information Engineering and Ph.D. degree in System Engineering from School of Electronic and Information, Xi'an Jiaotong University, Xi'an, China, in 2003 and 2010, respectively. Currently, he is an assistant professor of the Systems Engineering Institute, Xi'an Jiaotong University. His research interests include Smart Grid, network security and trustworthy software.

**Yanan Sun** received her B.S. degree in Information Engineering and M.S. degree in Systems Engineering from School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China, in 2011 and 2014, respectively. Currently, she is a Ph.D. student at University of British Columbia, Vancouver, Canada. Her research interests include cyber-physical systems, smart grid, network security and user privacy.

**Yang Liu** received his B.S. degree in automation from Xi'an Jiaotong University, China, in 2012. He is currently working toward his Ph.D. degree at the Systems Engineering Institute, Xi'an Jiaotong University, China. His research interests include Smart Grid, cyber-physical systems, and network security.



**Yuhong Gui** received her B.E. degree in Electrical Engineering and Automation from Xi'an Jiaotong University, Xi'an, China, in 2013. She is currently working toward her M.S. degree at the Systems Engineering Institute, Xi'an Jiaotong University, China. Her research interests include smart grids, power system technology and cyber-physical systems.

**Yucheng Zhao** received his B.S. degree in Automation from School of Electronic and Information, Xi'an Jiaotong University, Xi'an, China in 2014. Currently, he is a PhD candidate in the department of Industrial and Manufacturing Systems Engineering in the University of Hong Kong. His research interests include the green industry and holon manufacturing systems.

**Dai Wang** received his B.S. degree from School of Electrical Engineering, Xi'an Jiaotong University, Xi'an, China in 2006. Currently, he is a PhD student in Systems Engineering Institute, Xi'an Jiaotong University. He is also a visiting student researcher in the Department of Electrical Engineering and Computer Science (EECS), University of California, Berkeley, from 2014 to 2015. His research interests include Smart Grids, Integration of Renewable Energies and Cyber-physical System.

**Chao Shen** (S'09) received the B.S. and M.S. degrees in automatic control from Xi'an Jiaotong University, Xi'an, China, in 2007 and 2009, respectively, and his Ph.D. degree in system engineering from Xi'an Jiaotong University, Xi'an, China, in 2014. He is currently an Assistant Professor in the School of Electronic and Information Engineering, Xi'an Jiaotong University of China. His research interests include insider/intrusion detection, behavioral biometric, and measurement and experimental methodology.