Dynamic Data Injection Attack Detection of Cyber-Physical Power Systems with Uncertainties

Wang, Huaizhi; Ruan, Jiaqi; Zhou, Bin; Li, Canbing; Wu, Qiuwei; Raza, Muhammad Qamar; Cao, Guang-Zhong

Published in:
IEEE Transactions on Industrial Informatics

Link to article, DOI:
10.1109/TII.2019.2902163

Publication date:
2019

Document Version
Peer reviewed version

Link back to DTU Orbit

Citation (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain.
- You may freely distribute the URL identifying the publication in the public portal.

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.
Dynamic Data Injection Attack Detection of
Cyber-Physical Power Systems with Uncertainties

Huaizhi Wang, Member, IEEE, Jiaqi Ruan, Bin Zhou, Senior Member, IEEE, Canbing Li, Senior Member, IEEE,
Qiwei Wu, Senior Member, IEEE, Muhammad Qamar Raza, Member, IEEE, Guang-Zhong Cao, Senior Member, IEEE

Abstract—Understanding potential behaviors of attackers is of paramount importance for improving the cyber-security of power systems. However, the attack behaviors in existing studies are often modeled statically on a single snapshot, which neglects the reality of a dynamically time-evolving power system. Accordingly, a dynamic cyber-attack model with local network information is proposed to characterize the typical data injection attack with the integration of potential dynamic behaviors of an attacker. The proposed model collaboratively alters the meter measurement in a stealthy way to illegally contaminate the system state, thus posing severe threats to cyber-physical power systems. We then develop a novel anomaly detection countermeasure from the perspective of state estimation to effectively recognize the dynamic injection attack. In this countermeasure, an interval state forecasting method is proposed to approximate the possible largest variation bounds of each state variable based on a worst-case analysis considering the forecasting uncertainties of renewable energy sources, electric loads, and network parameter perturbations. In addition, the kernel quantile regression is introduced and implemented to formulate the uncertainties in renewable energy and electric load forecast as a series of confidence intervals. When any state variable falls outside its pre-forecasted intervals, the proposed countermeasure detects the anomaly and sets an alarm condition indicating the possibility of data contamination. Finally, the results from our extensive studies on several IEEE standard test systems have been presented to demonstrate the feasibility of the dynamic attack and the effectiveness of the detection countermeasure.

Index Terms—Cyber physical power system, interval state estimation, cyber-attack, kernel quantile regression, false data injection attack.

I. NOMENCLATURE

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm</td>
<td>Boolean number with false/true value</td>
</tr>
<tr>
<td>Gij, Bij</td>
<td>Conductance and susceptance of the i-j branch</td>
</tr>
<tr>
<td>Gbr, Bbr</td>
<td>Conductance and susceptance of the br-th line</td>
</tr>
<tr>
<td>Gbus, Bbus</td>
<td>Nominal values of conductance and susceptance</td>
</tr>
<tr>
<td>K(r1, r2)</td>
<td>Kernel function with input r1 and r2</td>
</tr>
<tr>
<td>Lo, Qlo</td>
<td>Active- and reactive power load of the i-th local load point at the r-th snapshot</td>
</tr>
<tr>
<td>N</td>
<td>Number of training samples</td>
</tr>
<tr>
<td>O</td>
<td>Logic OR operation</td>
</tr>
<tr>
<td>Pr, Qr</td>
<td>Optimal active and reactive power injections of the i-th bus at the t-th snapshot</td>
</tr>
<tr>
<td>Pr, Qr</td>
<td>False active and reactive power injections</td>
</tr>
<tr>
<td>Prij, Qrij</td>
<td>Active and reactive power flows of the i-j branch</td>
</tr>
<tr>
<td>Plij, Qlij</td>
<td>Power flows of the l-th branch</td>
</tr>
<tr>
<td>Pij, Qij</td>
<td>False data injections on power flows</td>
</tr>
<tr>
<td>Pij, Qij</td>
<td>Active and reactive output of the k-th generator</td>
</tr>
<tr>
<td>Pij, Qij</td>
<td>Optimal power generations</td>
</tr>
<tr>
<td>Ploss, Qloss, Plossmax, Qlossmax</td>
<td>Lower and upper generation limits</td>
</tr>
<tr>
<td>Fl</td>
<td>Power loss</td>
</tr>
<tr>
<td>Floss data injections on power generation</td>
<td></td>
</tr>
<tr>
<td>sij, (sij,1)</td>
<td>Capacity limits of reactive power generation</td>
</tr>
<tr>
<td>f(t), f(t)</td>
<td>Apparent power limits of the l-th branch at n-th and (n-1)th snapshots</td>
</tr>
<tr>
<td>Smax</td>
<td>Maximal apparent power limits</td>
</tr>
<tr>
<td>Vmin, Vmax</td>
<td>Total number of snapshots in dynamic attack</td>
</tr>
<tr>
<td>Vmin, Vmax</td>
<td>Lower and upper limits of voltage magnitude</td>
</tr>
<tr>
<td>x*</td>
<td>Falsified voltage magnitudes of the ij-th bus</td>
</tr>
<tr>
<td>t</td>
<td>A column vector</td>
</tr>
<tr>
<td>Cost functions of the rth active- and reactive power generators</td>
<td></td>
</tr>
<tr>
<td>Mapping function in kernel quantile regression</td>
<td></td>
</tr>
<tr>
<td>Vector functions that characterize the relationships between meter measurement and x</td>
<td></td>
</tr>
<tr>
<td>Lower and upper limits of the q-th quantile</td>
<td></td>
</tr>
<tr>
<td>A training sample with input v_i and output e_i</td>
<td></td>
</tr>
<tr>
<td>t</td>
<td>The r-th operating snapshot of power system</td>
</tr>
<tr>
<td>ω1</td>
<td>Control coefficient in state forecasting method</td>
</tr>
<tr>
<td>xjt</td>
<td>Optimal operating level of the yth state variable</td>
</tr>
<tr>
<td>xjt</td>
<td>Lower and upper variation limits of xjt</td>
</tr>
<tr>
<td>xjt</td>
<td>Real state value from traditional state estimator</td>
</tr>
<tr>
<td>xjt</td>
<td>Boundary states on the edge of the attack area</td>
</tr>
<tr>
<td>xjt</td>
<td>Initial state values of the boundary states</td>
</tr>
<tr>
<td>xjt</td>
<td>Operating state variables at the t-th snapshot</td>
</tr>
<tr>
<td>xjt</td>
<td>Local measurement vector in attack area</td>
</tr>
<tr>
<td>Model parameters in mapping function</td>
<td></td>
</tr>
<tr>
<td>Maximal deviations from nominal conductance and susceptance</td>
<td></td>
</tr>
<tr>
<td>Real deviations from nominal parameters</td>
<td></td>
</tr>
<tr>
<td>Uncertainties of power injections at bus i</td>
<td></td>
</tr>
<tr>
<td>Uncertainties of power injections at bus i</td>
<td></td>
</tr>
<tr>
<td>Uncertainty of renewable power generation</td>
<td></td>
</tr>
<tr>
<td>Lower and upper limits of the uncertainty Δui</td>
<td></td>
</tr>
<tr>
<td>Upper limits of the entire active load variations.</td>
<td></td>
</tr>
<tr>
<td>Upper variation limits of total reactive load, conductance, susceptance and renewables</td>
<td></td>
</tr>
<tr>
<td>Lower and upper variation limits of active- and reactive power consumptions at the t-th bus</td>
<td></td>
</tr>
<tr>
<td>Increment of power loss</td>
<td></td>
</tr>
</tbody>
</table>

This work is supported in part by the National Natural Science Foundation of China (51877072, U1813212, 51707123, 51507056), and in part by the Shenzhen government fund (2017091910424276).

H. Wang, J. Ruan and G.-Z. Cao are with the Shenzhen Key Laboratory of Electromagnetic Control, College of Mechatronics and Control Engineering, Shenzhen University, Shenzhen 518060, China, (e-mail: wanghz@szu.edu.cn, jqruan01@163.com, gzcao@szu.edu.cn).

B. Zhou (Corresponding author) and C. Li are with the College of Electrical and Information Engineering, Hunan University, Changsha 410082, China (e-mail: binzhou@hnu.edu.cn, licanbing@gmail.com).

Q. Wu is with the Centre for Electric Power and Energy, Department of Electrical Engineering, Technical University of Denmark, Kgs. Lyngby 2800, Denmark (e-mail: qwu@elektro.dtu.dk).

Muhammad Qamar Raza is with the Power and Energy System group, at School of Information Technology and Electrical Engineering, University of Queensland, Brisbane, QLD 4072, Australia (e-mail: qamar.raza@uq.edu.au).
\( \Delta S_{lt} \) Incremental capacity limit of the \( l \)-th branch
\( \Delta y_{jt}, \Delta \bar{x}_{jt} \) Limits of the \( j \)-th state variable
\( \theta_{ij} \) Falsified phase angle of the \( i-j \) branch
\( \lambda \) Balance parameter in quantile optimization
\( \rho_{kt} \) Check function with respect to the \( k \)-th quantile
\( \sigma \) Control parameter related to kernel width.
\( \varphi_{s} \) A uncertainty term within \([-1,1]\)
\( \kappa \) Initial snapshot in dynamic attack
\( \tau \) Confidence level
\( \zeta, \eta \) Control parameters in quantile optimization
\( \mathcal{H}(x) \) Hilbert space in kernel
\( \Omega_{A} \) Target area for attack construction
\( \Omega_{L} \) Set of local branches to be overloaded
\( \Omega_{RE} \) Set of local renewable energy buses
\( \Omega_{S} \) Set of local state variables
\( \Omega_{Br} \) Set of local network branches
\( \Omega_{B} \) Set of local network buses
\( \Omega_{G} \) Set of local active and reactive generators

## II. INTRODUCTION

In recent years, researchers have made tremendous efforts to make maximum use of digital and computerized technologies to overcome the limitations of the traditional power grid. Specifically, the need to meet future demand in an environmentally friendly manner has led to an interest in sustainable energy [1]. Meanwhile, the incorporation of market-driven demand-side energy management and conservation, including electricity storage, is a significant enhancement to ensure reliable and efficient energy use. Large-scale deployment of real-time interactive technologies, i.e., wide-area measurement systems and automated substations, enable optimization of physical appliances. These unprecedented changes are driving the transformation of the traditional electric grid into a deeply intertwined cyber physical power system (CPPS) combining power management with a supporting cyber infrastructure [2]. The CPPS provides a new paradigm for intelligently integrating the behaviors and decisions of all participants in the energy supply chain in order to deliver reliable, economical, and secure electrical energy. However, the CPPS also relies greatly on the supporting cyber assets and has been proven to be vulnerable to cyber-attacks, which pose severe threats to the countries involved [3].

Research related to cyber-attacks on CPPS fall into two categories. Papers in the first category suggest how to construct optimal stealth attacks on the basis of daily reports showing power flows and network connectivity [4]. False data injection attacks [5], denial of service attacks [6], load redistribution attacks [7], time synchronization attacks [8], resynchronization attacks [9] and outage attacks [10] have all been put forward to accomplish numerous malicious objectives. However, most existing attack strategies are generally built on a single snapshot, i.e., the operating states of CPPS at a given moment, which comes up with two practical issues. First, they may be inappropriate for handling the operation dynamics of an ever-changing power system [11] due to the variation of electric loads, output uncertainties of renewable energy sources and the preference from system operators. Second, they may bring in radical changes in meter measurements because time series characteristics in system states are usually omitted.

Consequently, such attacks on a single snapshot may trigger protection and response actions in CPPS to clear the cyber threats, mitigating security risks and ensuring compliance with physical regulations. Therefore, it is far more likely that attackers would design the attack strategies on multiple snapshots with consideration of CPPS dynamics. Thus, an in-depth understanding of cyber-attack with power system dynamics is helpful in identifying potential deceptive behaviors from the perspective of attackers. It can further help to design and implement appropriate prevention measures.

The second kind of research dissects the countermeasures for detecting and defending cyber-attacks from the standpoint of communications, physical, and system security. Communication security uses protocol [12], encryption and authentication [13] to prevent unauthorized access and provide trustworthy information interlinks between geographically distributed resources. Physical security refers to the optimal deployment of protective measurements for maintaining network observability and ensuring that the grid is immune from well-coordinated attacks [14]. System security broadly employs statistical [15] and non-statistical methods [16] to identify anomalies with legacy equipments. Nevertheless, these countermeasures depend either on redundant sensors and communication channels or fit only a specific grid topology. These existing countermeasures also assume, improperly, the nature and type of the attacks. For instance, the method in [17] introduced the honeypot as a decoy system to address the denial of service attack and developed a strategic game theory to analyze the zero-sum interactions between attackers and defenders. A model-based mitigation algorithm was designed in [18] to defend against data integrity attack on automatic generation control. Also, a robust time-synchronization protocol using graph theory was proposed and applied to perform anomaly detection of Sybil attack in CPPS sensor network [19]. Apparently, these countermeasures were designed to protect CPPS from a given unchanged cyber-attack and they are, therefore, incapable of adapting to evolving cyber threats. In addition, the performance of the most of existing countermeasures may rely on pre-trained thresholds [15], which are fixed without consideration of changing operational scenarios and environmental noises. Hence, a new countermeasure that overcomes these shortcomings is urgently needed to enforce the cyber security of CPPS.

In summary, it is a pressing need for us to analyze the dynamic attack behaviors in CPPS and develop a new countermeasure for defending against dynamic cyber-attacks. However, in reality, attack behaviors vary from time to time due to the attainable knowledge and diverse attack objectives. For example, attackers may fail to penetrate a target system at first due to their limited information and then search for alternative solutions by invading the system step by step until they succeed [20]. Also, the behaviors may change substantially from attacker to attacker, both quantitatively and qualitatively, according to the different selected strategies, hacking tools and technical skills [21]. Therefore, it is impossible to develop a generic dynamic attack model to encompass all types of attacks and behaviors. In the recent past, false data injection attack (FDIA) has attracted a lot of research attention [4]. Different from other types of attacks, such as DoSA and jamming, FDIA can circumvent conventional bad data detection and
intrude the power system without being noticed. It is a typical cyber-attack capable of disturbing the power system state, making either physical, such as outage, or economic impacts on CPPS. Therefore, this paper takes FDIA as an example to illustrate the importance of dynamic behavior modeling of cyber-attack and its detection countermeasure.

In this paper, a new dynamic data injection attack model is firstly proposed with the integration of CPPS operational dynamics. We then design a novel holistic countermeasure to protect CPPS from unauthorized threats on the inside and malicious attacks on the outside. Compared with similar studies, our contributions are mainly threefold. First, we propose, for the first time, a new bi-level dynamic data injection attack model over multiple operation snapshots. The lower layer simulates power system local dynamics through optimal power flow (OPF) and estimates the optimal operating conditions of CPPS. The upper layer determines the minimal set of meters required to be contaminated in the attack area and thus characterizes potential behaviors of attacker. Second, we propose an novel interval state forecasting method to numerically approximate the possible largest deviations of all state variables. This method exploits the temporal correlation in nodal states and takes into account the forecasting uncertainties of renewable energy, electric loads, and network parameter perturbations. We formulate the forecasting uncertainties and parameter perturbations as statistical confidence intervals by using kernel quantile regression. Third, we design a new security countermeasure from the perspective of CPPS state estimation to detect meter anomalies and ensure data integrity. For each state variable, any deviation that does not fall within its pre-forecasted intervals is flagged as an anomaly state that indicates a high possibility of data tampering. Comprehensive and extensive experiments with several IEEE benchmarks have been implemented to demonstrate the viability of our dynamic data injection attack and the high-efficiency of the detection mechanism. The numerical results reveal the vulnerabilities of CPPS and further underscore the urgency of defending against malicious hidden cyber-attacks.

III. PROPOSED DYNAMIC DATA INJECTION ATTACK MODEL

In order to evade the residual test in dispatch center, several practical issues should be considered in the modeling of a synthetic data injection attack. First, the attack strategy should use the underlying AC grid model because a DC-based attack model may contribute a perceptible residual to the power system state estimation [22]. Additionally, the existing research commonly assumes that attackers possess detailed global information on the target, including comprehensive topology, load data, and branch parameters. In reality, this information is both volatile and protected within a power dispatch center. Access to all such global information for formulating an attack is both expensive and unrealistic. It is far more likely that an attacker would have only limited local information [23]. Moreover, attackers tend to focus their efforts to minimize the number of altered meter measurements, i.e., the monitored parameters, as more widespread changes increase the risk of detection. Hence, most attackers use highly sparse attack strategies requiring minimal effort in the real world [24]. Most importantly, the published FDIA strategies are static, generally conducted against a single snapshot of the grid, which does not reflect the reality of a dynamic, changing operational power system [11]. Consequently, we take into account all above practical issues and originally propose a bilevel dynamic data injection attack strategy on multiple operational snapshots according to the following equations:

Objective: \[ \min \sum_{i=1}^{\kappa} \sum_{t=1}^{T} \left( x_{i,t} - h_{i,t} (x) \right)^2 \] (1)

subject to:

\[ P_{Gt}^* + P_{Ft}^* = \sum_{j \in O} \sum_{j \in o} (V_{i} V_{o}^*) (G_{ij} \cos \theta_{ij} + B_{ij} \sin \theta_{ij}) \] (2)

\[ Q_{Gt}^* + Q_{Ft}^* = \sum_{j \in O} \sum_{j \in o} (V_{i} V_{o}^*) (G_{ij} \sin \theta_{ij} - B_{ij} \cos \theta_{ij}) \] (3)

\[ P_{Gt}^* + P_{Ft}^* = -\left( V_{i}^2 - V_{o}^2 \right) (G_{ij} \cos \theta_{ij} + B_{ij} \sin \theta_{ij}) \] (4)

\[ Q_{Gt}^* + Q_{Ft}^* = \left( V_{i}^2 - V_{o}^2 \right) (G_{ij} \sin \theta_{ij} - B_{ij} \cos \theta_{ij}) \] (5)

\[ V_{\min} \leq V_{i} \leq V_{\max} \] (6)

\[ P_{Gt}^* \leq P_{Gt}, \quad Q_{Gt}^* \leq Q_{Gt}, \quad P_{Ft}^* \leq P_{Ft}, \quad Q_{Ft}^* \leq Q_{Ft} \] (7)

\[ \sqrt{\left( P_{Gt}^* + P_{Ft}^* \right)^2 + \left( Q_{Gt}^* + Q_{Ft}^* \right)^2} \leq S_{i} + \Delta S_{i} \] (8)

\[ S_{i} + \sum_{t=1}^{\kappa} \sum_{q=1}^{N} \Delta S_{q} \geq S_{i} \] (9)

\[ \{ P_{Gt}, Q_{Gt} \} = \arg \min \sum_{i=1}^{\kappa} \sum_{t=1}^{T} \left( f_{i,t} (P_{Gt}) + f_{i,F} (Q_{Gt}) \right) \] (10)

where \( \kappa \leq t \leq \kappa + T \), which indicates that the dynamic data injection attack will be implemented on \( T \) snapshots in CPPS. Six types of parameters, i.e., \( P_{G}, Q_{G}, P_{F}, Q_{F}, P_{G}, \) and \( Q_{G} \), are the unknown elements that are required to be solved in each snapshot to constitute the attack vector, resulting in a set of biased states, \( \theta_{ij} \) and \( V_{i} \). The attack target area \( \Omega \) is defined beforehand according to the interest and knowledge of the attackers. In addition, the thermal limits of several given lines are set to small values at the initial snapshot. These limits linearly increase as shown in (9).

The objective function (1) is defined to minimize the total number of nonzero elements in the attack vector for all snapshots. The attack vector obtained from (1)-(10) may consist of many small-valued nonzero elements in practice. We treat these elements as zero if their values are within the variation tolerances of measurement noise [25]. The power injection models (2)-(3) and power balance models (4)-(5) describe the AC grid model subject to bus voltage operational limits (6) and generator capacity limits (7). To make the attack more realistic, we assume that the attacker’s objective is to overload several given lines gradually as defined in (8)-(9) [26]. In addition, (10) specifies that the values of the boundary states should remain unchanged before and after the implementation of the attack [27]. OPF is performed locally according to (11), subject to power balance constraints (12)-(13), generator capacity limit (14), voltage operation limits, thermal limits (15) and power flow constraints.

According to the proposed dynamic data injection attack
modeling strategy (1)-(15), the attacker first performs local OPF to estimate the steady state values of the attack area, and then constructs optimal dynamic attack vectors over multiple operational snapshots by solving the upper level L0-norm minimization problem in (1)-(10). Four types of local information, i.e., historical load profiles, generation cost, network parameters and topology, are required for dynamic data injection attack formulation. It seems that the information for dynamic attack is extensive. However, in reality, the required information in (1)-(15) is greatly reduced when compared to the required information for global attack [7]. In our dynamic data injection attack model, the information required for attack construction belongs to local information and so any information outside of the attack area is unnecessary. Furthermore, the proposed dynamic attack model made no assumption on the attack area and thus the attacker is free to choose any subnetwork with accessible load profiles, network parameters and topology as the attack region. Moreover, the generation cost information is not necessary anymore if none of the generators exists in this attack region. Therefore, it is clear that the proposed dynamic data injection attack model with limited local network information is relatively more practical than the attacks with global information [22].

Once the attack vectors are obtained by solving (1)-(15), the attacker should implement the attack vectors sequentially over multiple operational snapshots. Each data injection attack vector represents the changing values of all contaminated meters at a given snapshot. The time interval of two adjacent snapshots are exactly the time interval between two data injection attacks. The launch of an attack vector may have time delays and will be completed within several seconds as measurement data is transmitted at this time scale. A typical time delay inside the injection attack will not affect the attack performance because the delay is much less than the time interval of two consecutive snapshots, generally at a minute level. After all attack vectors have been implemented, the target lines will be overloaded without being detected, which may result in a cascading failure of the target power grid. Compared to the existing attack models, the most prominent feature of the proposed attack model is the integration of CPPS dynamics into the attack model such that the meter measurement can be contaminated gradually. This feature avoids radical changes in meter readings and further reduce the chance of being detected.

IV. INTERVAL STATE FORECASTING WITH UNCERTAINTIES

In recently years, researchers have adopted statistical and non-statistical tests for attack detection from cyber-attacks [28]. However, the application of these methods may be severely limited in reality because of the following two reasons. First, the performance of these methods may rely on several pre-trained thresholds [29] that are difficult to tune due to their dependencies on system operating conditions and highly sensitive to the measurement and processing noise. Second, these methods may deal with attack detection problems as classification problems [30] and so fail to distinguish normal states from anomaly states. Therefore, recognizing the abovementioned deficiencies, we focus on the security features of CPPS state estimation and consequently propose a new generic anomaly detection countermeasure. This countermeasure originates from a novel interval state forecasting method that are used to approximate the common largest deviations of any state variable, as presented in this section. The proposed attack detection countermeasure is given in section V.

A. Overall Interval State Forecasting Framework

Electricity demand changes continuously over time according to weather, human schedules, and economic factors and exhibits apparent time-series characteristics. These characteristics result in a temporal correlation between system nodal states [31]. This indicates that the nodal states can be forecasted with only small deviations. Thereby, we propose a novel interval state forecasting method to numerically evaluate the common largest deviations of state variables. This method consists of four main parts: CPPS uncertainties modeling, deterministic state assessment, state uncertainty modeling, and interval state formulation. Fig. 1 illustrates the overall framework of the method.

The CPPS uncertainties modeling component documents model parameter perturbations and forecasting uncertainty evaluation of renewable energy and electric load. The uncertainty information is used to determine the bounds of state variable uncertainties. In addition, the deterministic state assessment phase computes median values for all state variables by applying economic dispatch and OPF to accommodate supply and forecasted loads. Combining the state uncertainty information with the deterministic state values produces the final outer operating intervals for all state variables, as described in the interval state formulas. The details of the remaining subparts are given in [15].

B. CPPS Uncertainties Modelling

Power system networks operate, by design, at an optimal level when the system load is met at the possible lowest cost, subject to the transmission constraints and equipment operating limits. System uncertainties make deviations from the optimal level inevitable. The modeling of these uncertainties helps quantify the common largest deviations from a well-planned operating level. Perturbations in the power network parameters [32] and the difficulty of forecasting renewable energy and electric demand [33] are two primary contributors to the uncertainties. We now elaborate on these factors.

1) Network parameter perturbations: Recent research often assumes that the values of network parameters are known precisely. However, practically, these values vary in practice according to weather conditions, environmental changes and
equipment aging. To accommodate this reality, we consider all network parameters to be variable within specific bounds [32], described as follows,

\[ G_{\text{in}} = G_{\text{nom}} + \Delta G_{\text{in}}, e_0 \]

\[ B_{\text{in}} = B_{\text{nom}} + \Delta B_{\text{in}}, e_0 \]

Apparently, the conductance and susceptance, i.e., \( G_{\text{in}} \) and \( B_{\text{in}} \), are the sum of their respective nominal values, denoted as \( G_{\text{nom}} \) and \( B_{\text{nom}} \), and uncertainty terms.

2) Forecast uncertainty modeling: Usually, uncertainties with regard to forecasting electric load and renewable energy are typically modelled with a parametric Gaussian, Beta and Weibull distribution [33]. However, these modeling methods may not be accurate as they ignore the fact that the forecast uncertainty varies with the level of the forecast outputs [34]. In other words, it is more appropriate to model the forecasting error of a renewable energy or electric load as a conditional probability distribution varying with its output level. Therefore, we implement a kernel quantile regression in this paper to statistically estimate the conditional forecasting distributions. Kernel quantile regression [35] is an extension of linear quantile regression and acts as an effective tool for exploratory data analysis. It uses nonlinear kernels to learn a stochastic conditional dependency of response variable given the predictor variables. Simply speaking, the kernel quantile regression is a statistical technique that estimate the conditional quantiles from a set of input-output training samples.

Considering a set of training samples \((r_1, e_1), \ldots, (r_N, e_N)\), with input \( r_i \in \mathbb{R}^d \), output \( e_i \in \mathbb{R} \) and number of samples \( N \), the kernel quantile regression specifies that the non-linear quantiles of the conditional distribution of the output \( e \) given input \( r \) can be typically formulated in term of the following optimization:

\[
\min_{\beta} \sum_{i=1}^{N} \rho_{\tau} (e_i - g(r_i)) + \lambda \left\| \beta \right\|_1/2
\]

where the Hilbert space \( \mathcal{H}_K \) is defined by a reproducing kernel function \( K(r_1, r_2) \). The check function \( \rho_{\tau} \) with respect to the \( \tau \) quantile is described as follows:

\[
\rho_{\tau} (e_i - g(r_i)) = \begin{cases} 
\tau (e_i - g(r_i)) & \text{if } e_i \geq g(r_i) \\
(\tau - 1)(e_i - g(r_i)) & \text{if } e_i < g(r_i)
\end{cases}
\]

One of the key problems with respect to (18) is how to define the mapping function \( g \). Here, we apply the representor theorem to formulate the mapping function as a linear function of the kernel \( K(r_1, r_2) \):

\[
g_r(r) = \sum_{i=1}^{N} \beta K(r, r_i) / \lambda + \beta_0
\]

Any smoothing, additive or interactive spline model can be taken as the kernel function \( K(r_1, r_2) \) because these functions all have the reproducing property. In this study, a radial basis function is implemented as the kernel function, as follows:

\[
K(r_1, r_2) = \exp(-\|r_1 - r_2\|^2/2\sigma^2)
\]

Given the confidence level \( \tau \), we transform the optimization problem (18) into a quadratic programming model by taking (19)-(21) into (18), as detailed below [35]:

\[
\min \sum_{i=1}^{N} \xi_i + (1-\tau) \sum_{i=1}^{N} \eta_i + \lambda \sum_{i=1}^{N} \beta_i^2
\]

s.t.

\[
e_i - \beta_0 - \sum_{i=1}^{N} \beta_i K(r, r_i) / \lambda \leq \xi_i
\]

\[
\beta_0 + \sum_{i=1}^{N} \beta_i K(r, r_i) / \lambda - e_i \leq \eta_i
\]

\[
\xi_i \geq 0, \eta_i \geq 0
\]

where the model parameters \( \beta_i \) \((0 \leq i \leq N)\) in the mapping function are unknown, and are required to be solved.

Karush–Kuhn–Tucker (KKT) condition theorem [36] is used here to solve the minimization problem (22)-(25). As far as \( \beta_0 = \beta_N \) are known, the error distribution for forecasting of electric load or renewable power can be modeled statistically as an interval curve, with lower and upper limits, as follows:

\[
q_r^{\tau} = \sum_{i=1}^{N} \beta_i \exp\left(-\frac{-\|r - r_i\|^2}{2\sigma^2}\right) / \lambda + \beta_0
\]

\[
q_r^{\tau} = \sum_{i=1}^{N} \beta_i \exp\left(-\frac{-\|r - r_i\|^2}{2\sigma^2}\right) / \lambda + \beta_0
\]

In this paper, we use kernel quantile regression to analyze the stochastic dependence of the forecasting error of electric load or renewable power on the real output level. Therefore, the real output levels are fed as the input parameters \( r \) of the training sample in (22)-(25), and the point forecast errors are taken as the output \( e \). As a result, from (26)-(27), we can conclude that the uncertainty for forecasting of electric load or renewable power is able to be formulated as a nonlinear quantile curve with lower and upper bounds. Compared with conventional linear quantile regression, the main benefit of the kernel quantile regression attributes to its strong capability for formulating the highly nonlinear dependence of the forecast error on its output level. Such thorough formulation of the forecast error distribution makes the accurate quantification of the variation bounds of power system state variables possible.

C. Deterministic State Assessment

This subsection presents the method for determining optimal operating values for all system state variables. We collect real-time generation schedules, electric load forecasts, renewable power forecasts, and the current network topology and operating conditions as they are available from real-time electricity markets or the topology estimator. We provide this information as input parameters to economic dispatch. Then, economic dispatch is performed by applying an interior point method to set specific output levels for each existing generation facility to produce and supply energy at the lowest cost and greatest reliability. Any operating limits of generation and transmission facilities should be accommodated in this process. Thereafter, with the generation set points from economic dispatch, we solve the power flow problem iteratively using the Newton–Raphson method to determine the power flows and bus voltages throughout the grid. The power flow solutions give the predicted optimal values for all state variables, including voltage magnitudes and phase angles, based on the renewable energy and electric load forecasts. These calculated values of the state variables are later used for interval state estimation in CPPS.

D. State Uncertainty Modelling

In general, the deterministic state assessment approximates the optimal operating levels for all state variables. In practice, the optimal operating levels for all state variables fluctuate due to the ever-present uncertainties from model parameter perturbations and forecasting errors. Similarly, any cyber-attack on meter measurements and communication channels will not doubt degrade the temporal correlation in nodal states, and thus increase the deviations from their well-planned optimal levels [37]. Therefore, we develop a new state uncertainty modeling method to distinguish normal fluctuations from
anomalies caused by cyber-attacks. This method implements a worst-case analysis to approximate the largest regular deviation for each normal state and thus ensure a high degree of confidence in identifying anomaly states. Mathematically, we model the outer variation bounds of each state variable in each interval as a dual nonlinear programming problem [38], considering the forecasting uncertainties and network parameter perturbations as follows:

\[
\begin{align*}
\text{Objective:} & \quad \left[ \Delta x_g, \Delta \bar{x}_g \right] = \left[ \min \varepsilon_i^T \Delta \bar{x}_i, \min -\varepsilon_i^T \Delta \bar{x}_i \right] \\
\text{s.t.} & \quad P_g' + \Delta P_{g,Di} - \Delta P_{Di} = \sum_{j=\Omega_G} V_j \left( G_{ij} \cos \theta_{ij} + \text{B}_{ij} \sin \theta_{ij} \right) \\
\text{and} & \quad Q_g' + \Delta Q_{g,Di} - \Delta Q_{Di} = \sum_{j=\Omega_G} V_j \left( G_{ij} \sin \theta_{ij} - \text{B}_{ij} \cos \theta_{ij} \right)
\end{align*}
\]

Equation (40) describes the regular state deviation caused by system uncertainties. With the aid of these forecasted outer bounds, a novel attack detection countermeasure is originally proposed, as presented in the following Section.

V. ANOMALY DETECTION COUNTERMEASURE

Evidently, falsified measurements injected by malicious dynamic data injection attack would appear to degrade the temporal correlation in nodal states and cause deviations from the norm. While, in practice, we can forecast the regular largest deviations for each state variable according to (40). As a consequence, at a given moment, any estimated state from traditional state estimator falling outside the pre-forecasted intervals suggests that the estimated state cannot be trusted anymore. It further indicates that current measurement information has been contaminated by an attack. Therefore, an anomaly alarm for data tampering should be raised when this occurs. These analyses constitute the attack detection countermeasure we propose, mathematically described as:

\[
\text{Alarm} = O \left( \hat{x}_g \not\in \left( \Delta \bar{x}_g, \bar{x}_g \right), \quad \gamma \in \Omega_G \right)
\]

Here, equation (41) means that any estimated state lying outside of its pre-forecasted intervals would trigger the Alarm, indicating a high possibility of data manipulating.

The flowchart of the attack detection countermeasure is presented in Fig.2. It consists of five main steps. First, we collect several historical load demand datasets, renewable power generation datasets and their corresponding forecast errors. For any dataset, we create a new training sample, normalize it and calculate its quantile curves based on kernel quantile regression according to (18)-(27). Second, the network nominal parameters and their perturbations are required to be determined. The above two steps are performed in an offline manner. In the third step, the optimal operating levels of all state variables are estimated, as presented in subsection IV-C. Afterwards, we observe the output levels for all load points and renewable energies, determine their corresponding variation ranges, and then approximate the lower and upper deviations of each state variable under a worst-case scenario based on (28)-(40). Finally, any state lying outside its pre-forecasted intervals is identified as an anomaly and the Alarm will be triggered with the aid of (41). Otherwise, the Alarm should not be raised. The last three steps are updated online in accordance with the time scale of state estimation in CPPS.

The novelty of this section is the proposal of a new generic cyber security method designed from the perspective of CPPS state estimation. This method originates from a novel interval state estimator, as presented in Section IV. It uses the worst-case analysis and takes the largest regular deviation of state variables into account to decide whether an estimated state is worth trustfulness or not. It is capable for detecting not only malicious injection attacks but also casual measurement errors, screening out various security issues. It should be noted that any normal state has a high confidence level for varying within its variation interval even there are errors simultaneously in network parameters, renewable generation predictions and load predictions. This is because the interval state estimator in our countermeasure assesses the possible largest devia-
tions of CPPS state under a worst-case scenario.

![Flowchart of anomaly detection countermeasure](image)

There are three main advantages of this approach. First, the proposed countermeasure requires significantly less investment. As an updated version of a traditional state estimator, it requires no additional protection and measurement equipment. Second, this countermeasure makes no assumptions concerning the network topology and nature of the attacks and therefore exhibits a better generalization capability. Third, the forecasted deviations in our countermeasure vary with the changing network state in real time. Thus, our proposed countermeasure exhibits better detection accuracy than statistical methods because the pre-trained thresholds in statistical methods are largely static and do not vary with the changing operating scenarios. The limitations of this approach are mainly twofold. First, our countermeasure is capable for triggering an alarm when any system state has been contaminated. However, it fails to clear the alarm and reconstruct the normal system states. Second, an alarm from our countermeasure is not necessarily a guarantee of that it comes from a malicious cyber-attack. In other words, the proposed countermeasure fails to distinguish cyber-attack with other possible outliers, such as that from unintentional manual error. How to solve these two limitations is our future research topic.

## VI. Case Studies

The feasibility and effectiveness of our dynamic data injection attack model and detection countermeasure have been validated with comprehensive tests on IEEE standard 30-, 57- and 118-bus systems having network topologies and line parameters are from [40].

### A. Investigation on Dynamic Cyber Attack

1) Experimental settings: All test systems, i.e., IEEE standard 30-, 57- and 118-bus systems, are fully observable with meter placements given in [41]. Two types of meters, including power injection meters and power flow meters are considered. We also installed two additional meters at the slack bus to measure the reference values for voltage magnitude and phase angle. To simulate real power system dynamics, we assumed all load points in the test systems follow four different daily load curves scaled down to match the load levels in the three test systems. We collected these daily curves from the Dongguan Power Supply Bureau of the Guangdong Power Grid in China. The dynamic data injection attack model proposed in this paper requires that attackers have the ability to obtain a local network information for the target system. Therefore, we select arbitrarily a subnetwork for each test system, as plotted in Fig. 3, and assume that attackers have obtained the complete information for these subnetworks and know nothing about the rest of the networks. In practical applications, the attack subnetworks can be chosen freely according to the target lines, interest of the attackers and difficulties in obtaining different local information.

The L0-norm objective aims to minimize the number of nonzero elements in the attack vectors. However, our experiments show that the attack vectors contain many small-valued elements. In reality, any element with the value below 1e-4 can be treated as a zero element because measurement noise also varies within this range. In addition, the L0-norm problem is difficult to solve, being NP-hard and nonconvex. We relax the L0-norm minimization to the L1-norm problem and solve it with YALMIP [42]. We implemented the proposed dynamic data injection attack with MATLAB R2014a on a PC with an i7-6700 3.4 GHz CPU and 32 GB of RAM.

2) Numerical results: We carried out simulations with a mix of operating snapshots. For the IEEE 30-bus system, we assumed that the dynamic attack was launched at 2:00 PM with the aim of overloading 2 transmission lines, i.e., 16-17 and 18-19 because overloading one line is insufficient to destabilize the power system due to the N-1 principle. The corresponding attack vectors over multiple operational snapshots are plotted as colorful ribbons in Fig.4(a). A ribbon graphically illustrates how an attack vector varies over all observable meters under a given snapshot. The attack vectors are obtained by solving the proposed dynamic data injection attack model (1)-(15). Under each snapshot, we also carry out the residue test in traditional state estimator to check whether the implemented attack can be detected or not. The resultant residuals are given in Fig.4(b). The time interval between two consecutive snapshots is set to 1 minute, which means that the time interval between two injection attack vectors is 1 minute. We also present the attack vectors at 9:00 PM and 10:00 AM as shown in Fig. 5 to demonstrate the feasibility of the dynamic data injection attack model in different load levels. In addition, the attack strategies for overloading lines 19-20 and 23-24 at 6:00 PM and 8:00 AM are given in Fig. 6. The dynamic data injection attacks with respect to IEEE 57- and 118-bus systems are shown in Figs. 7-8.

We designed our attacks to overload two lines, which may
be of very limited use in practice. As presented in Section III, the proposed attack model is able to overload multiple lines. Therefore, Fig. 9 plots the statistical attack magnitudes in IEEE 30-, 57- and 118-bus systems to demonstrate the extensive applications for overloading any given lines. In the left figure of Fig.9, cases 1-6 describe six attack samples with different operational scenarios for overloading 1 to 5 lines. In the right figure of Fig.9, the vertical coordinate represents the average of the sum of all meter changes. Ten different attack samples are considered. In addition, to analyze the solution efficiency of our dynamic data injection attack, Table I presents the statistics of the elapsed time required for solving (1)-(15). Six independent dynamic attack samples are considered for each test system. The elapsed time is obtained by calling the solve time function in YALMIP. Finally, to highlight the superior of the proposed dynamic attack model, our attack strategy is compared to conventional data injection attack via a series of simulations. The contaminated meters of several dynamic attack strategies as well as conventional data injection attacks on IEEE 30- and 57-bus systems are given in Table II. Meanwhile, we pick the three meters with the largest rate of change (RoC) for each test system. The RoCs of the three meters varied with the snapshots are plotted in Fig.10. In each snapshot, conventional data injection attack is assumed to be implemented with the same attack objective. The resultant RoCs of the three meters are also given for performance comparison. In Fig.10, the long- and short dash lines represent the RoCs of the contaminated meters from dynamic attack and conventional data injection attack, respectively.

Fig.4 Dynamic data injection attack to overload lines 16-17 and 18-19 at 2pm.

Fig.5 Dynamic attacks to overload lines 16-17 and 18-19 at 9pm and 10am.

Fig.6 Dynamic attacks to overload lines 19-20 and 23-24 at 6pm and 8am.

Table I

<table>
<thead>
<tr>
<th>IEEE Test system</th>
<th>Overloading lines</th>
<th>Dynamic data injection attack</th>
<th>Conventional data injection attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>30-bus system</td>
<td>5-6, 10-13, 25, 32-35</td>
<td>5, 6, 11-13, 19, 23, 32-35</td>
<td></td>
</tr>
<tr>
<td>57-bus system</td>
<td>5, 6, 8, 10-14, 25-26, 29, 31-35</td>
<td>5, 6, 8, 10-14, 19, 25-26, 29, 31-35</td>
<td></td>
</tr>
<tr>
<td>118-bus system</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table II

<table>
<thead>
<tr>
<th>No. of snapshots</th>
<th>No. of meters</th>
<th>Dynamic data injection</th>
<th>Conventional data injection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>161115</td>
<td>Dynamic data</td>
<td>Conventional data</td>
</tr>
<tr>
<td>2</td>
<td>161115</td>
<td>Dynamic data</td>
<td>Conventional data</td>
</tr>
<tr>
<td>3</td>
<td>161115</td>
<td>Dynamic data</td>
<td>Conventional data</td>
</tr>
</tbody>
</table>

Fig.7 Dynamic data injection attacks on IEEE 57-bus system.

Fig.8 Dynamic attack to overload 95-96 and 98-100 on IEEE 118-bus system.

Fig.9 Statistical dynamic data injection attacks for overloading multiple lines.

Fig.10 RoC curves of three typical meters varied with the snapshots.
3) Discussion: Fig.4(a) demonstrates that in order to physically overload two given lines, the attack vector changes across operational snapshots. The largest magnitudes of the manipulated meters in these attacks are around 0.25 p.u. Specifically, the attack vectors cover most of the meters with small magnitudes at the beginning of the snapshots. At this time, the attacks will not cause disruptive impacts on power system but slightly mislead the real power system states. In subsequent snapshots, these attacks contaminate few number of meters with relative large magnitudes and finally overload the given lines, posing severe consequences on power system. This is because the line capacities are configured to increase gradually to their real limits along with the snapshots so that the attack on each meter remains undetected. Therefore, power system dynamics should be considered in the modeling of attack behaviors, which is generally omitted in existing studies. This is the first major contributor of this paper. The numerical results from Fig. 4(b) prove that the residue have the same magnitude whether an attack is present or not, having values near 1.5e-8. This indicates that the dynamic attack succeeds in bypassing the traditional residue test and no security issue is revealed. Moreover, we checked the residues shown in Figs. 4-8 and found that none of the dynamic attacks had measurable effects on the residues. This further illustrates the effectiveness and feasibility of the proposed dynamic data injection attack model with local network information.

With reference to Figs. 4-5, the profiles of the attack vectors in different time periods are roughly similar to each other because the lines to be overloaded are the same. Conversely, for different overloaded lines, the attack profiles vary greatly across time periods, as shown in Figs. 5-6. This is understandable because our dynamic attack requires that different sets of meters must be contaminated cooperatively in order to circumvent the residue test in traditional state estimator while satisfying the underlying AC grid model. These conclusions are also true for IEEE 57- and 118-bus systems, as presented in Figs. 7-8. In addition, the largest magnitudes of the meters in the attacks on 57- and 118-bus systems are around 0.3 p.u. and 0.4 p.u., respectively. These meters are manipulated within 15 minutes. The manipulated magnitudes of the meters in each minute are relatively small, generally less than 0.1 p.u., and therefore, these dynamic data injection attacks cannot be detected by conventional bad data detector in power systems because they introduce no extra residuals. Furthermore, Fig. 9 shows that the sum of all meter changes, i.e., the total magnitudes of all manipulated meters, varies greatly along with the different lines to be overloaded. Meanwhile, the more lines to be overloaded, the harder it is to implement an attack with larger magnitudes. This means that the sparsity of dynamic data injection attacks is reduced when more lines are targeted for thermal attack.

Table I demonstrates that it takes an average time of 2.75s with a minimal of 1.46s and a maximum of 3.81s to solve the dynamic attack implemented in IEEE 30-bus system. With respect to IEEE 57- and 118-bus systems, the elapsed time corresponds to about 6.15s and 15.82s, respectively. It is obvious that the required time for attack construction is extended when system gets larger, as there are more equality and inequality constraints for dynamic attack formulation in more complex grids. Furthermore, it can be found that the time for attack construction in Table I ranges from 1.46s to 18.29s, less than the time interval for implementing an attack vector. This is because the NP-hard L0-norm optimization is relaxed into a L1-norm problem, which can be solved efficiently [43]. Therefore, our dynamic data injection attack model has a high solution efficiency and is applicable in the real world.

From Table II, it is obvious that the contaminated meters from dynamic data injection attack are very similar with the contaminated meters from conventional data injection attack. For example, only two meters are different in both attacks for overloading the line 15-23 in 30-bus system. This is because they have the same attack objective and similar attack formulations. However, we can see from Fig.10 that the RoCs of dynamic attacks are much smaller than the RoCs of conventional attacks. More specifically, all RoCs of dynamic attacks are below the 10%. While, most RoCs of conventional attacks are larger than the 10%. In other words, the contaminated meters of dynamic attacks have relatively smaller variations in each snapshot, when compared to the meters of conventional attacks. This is due to the fact that the dynamic attacks are implemented over multiple snapshots, while the conventional attacks are launched on only 1 snapshot. To overload the same given lines, conventional attacks have to falsify many meters in a single snapshot with large magnitudes. Vice versa, dynamic attack can slowly alter the meters over multiple snapshots. Therefore, it can be concluded that the proposed dynamic data injection model is superior to conventional data injection attacks. In a summary, the results in Figs. 4-10 and Tables I-II indicate that the attack behaviors exhibit a kind of dynamics and vary significantly in terms of operational scenarios, line locations, and grid topologies. Understanding these potential behaviors helps to reveal power system vulnerabilities and thus contribute to improvements in the cyber security of future smart grid.

B. Investigation on Detection Countermeasure

1) Experimental settings: We tested and benchmarked the effectiveness of the interval state forecasting-based anomaly detection countermeasures extensively. The countermeasures are cyclically performed every 15 minutes. The selection of the time interval for performing the countermeasure mainly relies on the types of attacks and the available information. Concretely, we choose this time interval for anomaly detection is because the proposed dynamic attack aims to bias real power system states that are estimated every 15-minutes in traditional state estimator. The state estimator provides accurate state estimation to many daily operational modules in the dispatch center, including optimal power flow and contingency analysis that use the same interval. We collected the forecasting errors and their output levels corresponding to renewable energy sources and electric loads from the energy management system in the Dongguan dispatch center. This forecasting error dataset covers all of 2016 with a 15-minute resolution. Afterwards, we modeled these errors over the training dataset as a series of variation quantiles based on a kernel quantile regression (18)-(27). We assumed all network parameters to have been varied within 5% in 15 minutes. We evaluated the...
optimal operating levels for all state variables using deterministic state assessment and calculated their corresponding variation bounds using state uncertainty modeling (28)-(39). Within these bounds, we determined the variation limits for each state variable from (40) and whether the countermeasure detected an anomaly according to (41).

2) Numerical results: We assumed that the dynamic attack vector from Fig. 4 for overloading lines 16-17 and 18-19 was launched on the IEEE 30-bus system. Fig. 11 presents the corresponding interval forecasting results. Figs. 12 and 13 give the interval results for detecting the two dynamic attacks for overloading lines 16-17 and 18-19 at 9:00 PM and 10:00 AM, respectively. We also implemented the dynamic attacks for overloading lines 25-30 and 30-31 on an IEEE 57-bus test system at 5:00 PM and 10:00 AM. Figs. 14 and 15 show the anomaly detection results. Fig. 16 shows the results corresponding to the attack given in Fig. 8 for an IEEE 118-bus system. In all of the preceding figures, the brown short-dashed line and the blue long-dashed line represent the upper and lower limits for the variations of state variables. The green star symbol denotes the normal states, while the red multiplication symbol denotes anomalous states, which indicate a high possibility of data manipulating in the measurement. In order to demonstrate the superior of the proposed countermeasure, the weighted least square, chi-square distribution test and the largest normalized residual test method [44] are also applied for detecting of anomalies from the dynamic data injection attacks in subsection VI-A. The results are partly shown in Table III. In this Table, the words ‘successful’ and ‘fail’ indicate that the corresponding method can or can’t recognize the embedded dynamic data injection attack. The detection results of the proposed countermeasure are also presented for performance comparison.

In order to analyze the solution efficiency of our anomaly detection countermeasure, the required time for performing the countermeasure is counted. Six cases for defending different dynamic attacks in a typical day are considered in each test system. We then obtain a series of statistics of the calculation time, as given in Table IV.
ing method and anomaly detection countermeasure account for the second and third contributors of this paper. Fig. 12 shows that the proposed countermeasure is also usable when the dynamic attack occurred at 9:00 PM. Figs. 11 and 12 show that their interval profiles are very similar, due to the attacks having the same objectives, i.e., overloading lines 16-17 and 18-19. Meanwhile, the intervals in Fig. 12 are noticeably smaller than the intervals in Fig. 11. This is due to the greater electric load uncertainties that existed at 2:00 PM. Figs. 11-13 also show that our proposed countermeasure reliably recognized various dynamic attacks in different operational scenarios having different objectives. Figs. 14-16 show that our countermeasure is also very effective for attack detection in IEEE 57- and 118-bus systems. Furthermore, the red multiplication symbols presented in Figs. 11-16 illustrate that our countermeasure remained effective irrespective of network topology. It is worth noting that the intervals of the phase angles differ relative to each other, i.e., the intervals of some phase angles were larger than others. This is due to the presence of the slack bus with fixed phase angles.

Tables III demonstrates that the weighted least square method and largest normalized residual method fail to recognize the dynamic attacks. These two methods are residual based algorithms. As presented in Fig.4(b), the dynamic data injection attack does not introduce any recognizable residual, making these two methods impossible for anomaly detection. In addition, Table III also shows that chi-square distribution test is unable to detect the abnormal conditions from dynamic attacks. This can be explained by the fact that the falsified measurement data actually satisfies the physical equations in power system. In contrast, the proposed countermeasure is very effective in all attack cases. We also checked the attacks shown in Fig. 9 and determined that any dynamic attack would have resulted in at least one anomaly state, which would indicate a success rate of up to 100% for dynamic attack detection. One reason accounts for this. The proposed countermeasure is a state forecasting aided detection method. Any condition that deviates from its predicted trajectory can be treated as an anomaly case. Note that we conduct the proposed countermeasure every 15-minutes in above simulations. This is because of the following three reasons: (1) it is designed based on state estimation, which are performed in power system in the same time interval; (2) it is used for detecting of the proposed dynamic attack, which will disrupt the power system by falsifying power system states; (3) the training samples for forecasting uncertainty modeling are collected in a 15-minutes interval. However, this countermeasure is very generic and thus can be also implemented in any time intervals of seconds, minutes and hours, if the training data with the same time interval is available.

In Table IV, we observe that it roughly takes 1 minute for solving our countermeasure (28)-(41) in IEEE 30-bus system. The time expenses for IEEE 57- and 118-bus systems amount to 3~4 minutes and 6~12 minutes, respectively. It is clear that the time required for the proposed countermeasure is less than 15-minutes. This means the calculation process of our countermeasure at a given operational scenario actually ends before the calculation of our countermeasure at the next scenario. Therefore, our countermeasure is applicable for anomaly detection in practical implementation. In addition, the solution efficiency of the proposed countermeasure can be further improved with the following measures: (1) Adopt more powerful personal computer; (2) Use sparse matrix and parallel technologies. This indicates our countermeasure is very attractive for various security applications in future deep cyber penetrated power system.

VII. CONCLUSIONS

In this research, an innovative dynamic attack model considering power system operational dynamics was proposed. Then, a new countermeasure was developed accordingly from the viewpoint of state estimation to recognize the existence of dynamic attacks in the system. In this countermeasure, we proposed a novel interval state estimator to approximate the uncertainties in state variables as a series of variation quantiles with a confidence level. We demonstrated the practicality and effectiveness of our dynamic attack model and detection countermeasure numerically in several IEEE standard test systems. The key findings from case studies can be summarized as: (1) Power system dynamics play an important role in stealthy attack construction and therefore should be considered for modeling of potential behaviors of attackers; (2) The proposed countermeasure based on interval state forecasting method is capable for detecting of anomaly states that lie outside the estimated state intervals, reliably raising an alarm condition when a dynamic attack is implemented. These two findings reveal an important vulnerability of CPPS and further highlight the urgency of updating traditional state estimator.

Our potential further work will focus on developing an automatic alarm clearing process. This process mainly contains three steps. At first, we will develop a deterministic state forecasting method with node-by-node correlation to correct the falsified states lying outside the interval. Then, a new coordinated bad data processor is required for reducing the smearing effect of cyber-attacks due to the undetected contaminated states. Finally, a fast bilinear state estimator will be applied to reconstruct the real power system state and automatically clear the alarm. Moreover, detecting the source of the resultant anomaly and improving the solution efficiency of our anomaly detection countermeasure are also considered as our further plans, making the real-time implementation of our countermeasure feasible.

REFERENCES


