This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2544854, IEEE Transactions on Smart Grid

A Bayesian Algorithm to Enhance the Resilience of WAMS Applications Against Cyber Attacks

Haris M. Khalid, *Member, IEEE* and Jimmy C.-H. Peng, *Member, IEEE*

***Abstract*— Monitoring critical infrastructures is highly dependent on the accuracy of the installed sensors and the robustness of estimation algorithms. Data-injection attacks can degrade the operational reliability and security of any cyber-physical infrastructures. An attacker can compromise the integrity of the monitoring algorithms by hijacking a subset of sensor measurements and sending manipulated readings. Such approach can result to wide-area blackouts in power grids. This paper considers several cases of severe data-injections with high probabilities of information loss. To achieve an accurate supervision, a Bayesian-based approximated filter (BAF) has been proposed at each monitoring node using a distributed architecture. To maintain a reduced communication overhead and time complexity, upper and lower bound methods have been developed. The performance of the proposed technique has been demonstrated in a mature synchrophasor application known as the oscillation detection. Two test cases have been generated to examine the immunity of the proposed estimation scheme in New Zealand and Oman power grids. The tests were conducted in the presence of harsh data-injection attacks and multiple system disturbances. Results show the proposed BAF method can accurately extract the oscillatory parameters from the contaminated measurements.**

***Index Terms*—Bayesian, cyber-physical systems, cyber security, data-injection attacks, inter-area oscillations, phasor measurement unit (PMU), power system monitoring, power system stability, real-time measurements, situational awareness, smart grid, synchrophasor, wide area monitoring system (WAMS).**

I. Introduction

DEPENDENCY of digital measurements for monitoring and control applications is increasing among the electrical power grids. The design of wide-area monitoring system (WAMS) has been recently introduced to improve the situational awareness of complex networks with the aim to further increase their transmission efficiency [1, 2]. The main purpose is to monitor network dynamics such as line loadings, voltage stability margins, and power oscillations [3,4]. Due to the complexity of the interconnected networks, the fast-changing operating conditions make the WAMS-based applications difficult to scrutinize the health of the incoming information. Such limitation makes a cyber-attack on the collected measurements as a potential threat [5]. In the meantime, the required energy and cost constraints restrict the deployment of the tamper-resistant hardware for the whole network. If a sensor is successfully attacked, its stored information can be compromised without any warnings. In the general literature, many methods have been proposed to mitigate the impacts of data-injection attacks in networked systems [6–8].

Given the importance of power systems in the context of national security, WAMS applications can be identified as an attractive attack target. It is far more challenging to detect malicious data-attacks as an adversary can choose the site of attack judiciously and design the attack data carefully [4, 9–11].

H. M. Khalid is with the Department of Electrical Engineering and Computer Science, Institute Center for Energy, Masdar Institute of Science and Technology (MI), Abu Dhabi, UAE. E-mail: harism.khalid.k@ieee.org, harism.khalid@yahoo.com

J.C.-H. Peng is with the Department of Electrical and Computer Engineering, National University of Singapore (NUS), Singapore. E-mail: j.peng@ieee.org

Acronyms and Abbreviations of Mathematical Formulations

BAF	Bayesian-based Approximated filter
DFC	Distributed Fusion Center
EO	Electromechanical Oscillation
PMU	Phasor measurement unit
WAMS	Wide-area monitoring system
x_t	state variable
$\mathbf{R}$	subspace
r	size of the state vector
F_t	model matrix of the state response
G_t	noise transition matrix
w	random process
t	time-instant
T	number of time-instants
χ_t^{ij}	Bernoulli random variable
N	number of PMU nodes
z	observation vector
p	number of synchrophasor observations
$h(.)$	nonlinear function
x	state matrix containing the system parameters
υ	observation noise
K	number of electromechanical oscillations
a	complex amplitude
σ	damping factor
f	oscillatory frequency
T_s	sampling time
b_k	complex amplitude of the k-th mode
$p(x)$	probability of distribution on oscillation state
$p(H)$	probability of distribution on observation matrix
z	data-injection free observation outputs
z_{pr}	predicted affected observation outputs
ΔH	perturbation in H
θ	gradient used to identify the perturbation
ψ	data-vector
K_{pr}	predicted gain matrix
R_e	Covariance of noise
$\tilde{K}$	optimal gain matrix
B	matrix of compatible dimensions
$P_{t+1\|t}$	estimated covariance matrix
Υ	covariance matrix of x_t
Π	covariance matrix of $\hat{x}$
U	unitary matrix
D	diagonal matrix
A, U, C, V	matrices of correct size
λ_{max}	maximum eigenvalue

In the recent literature, several methods have been proposed to identify abnormal data segments and isolate attacked sensors [12, 13]. However, most techniques have been published to enhance state estimation operations [14–18]. Few have been proposed for WAMS applications, and thus is the scope of this paper. Note state estimation updates the steady-state parameters of the grid, whereas WAMS applications focus on monitoring transient situations. False information could be given to delay control actions, which can result to system-wide blackouts [12, 19, 20]. Therefore, the motivation is to improve the capability of WAMS applications for mitigating and tolerating data-injection attacks.

Among WAMS applications, oscillation detection is one of the most mature and widely adopted function [2,3,21,22]. It has

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2544854, IEEE Transactions on Smart Grid

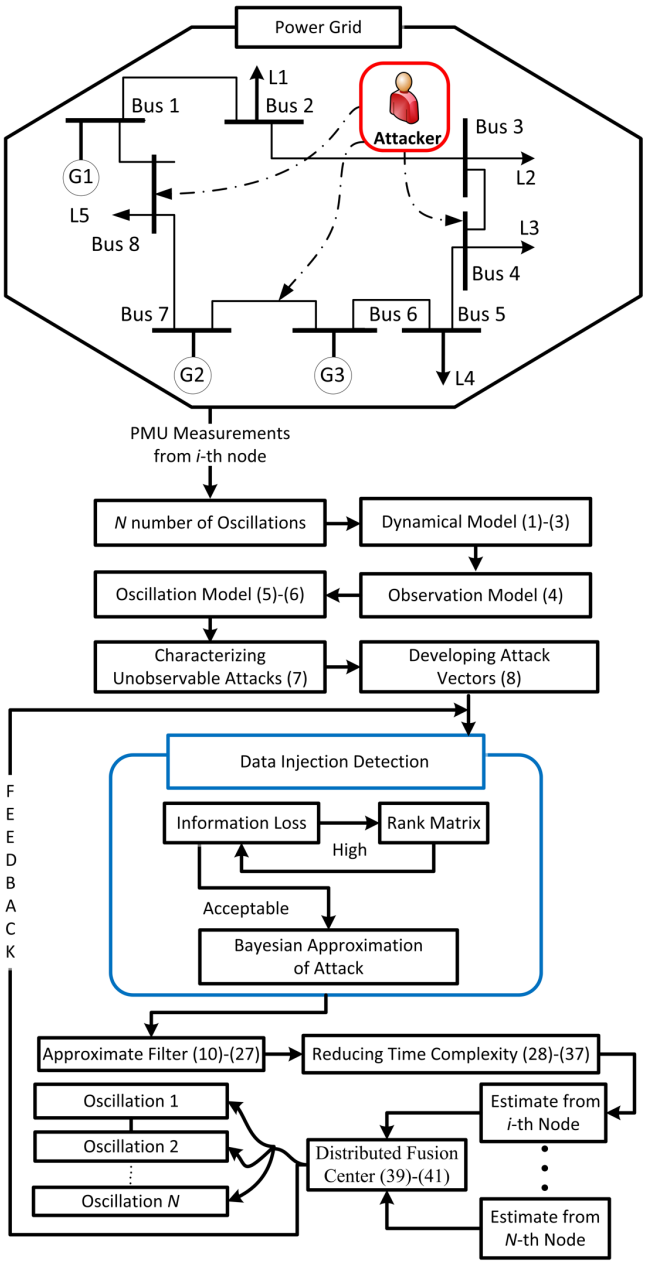

Fig. 1. Proposed data-injection immunity framework for WAMS application: an oscillation detection example

been installed in the control centers of many transmission utilities to monitor the damping of electromechanical oscillations in critical tie-lines. The damping dynamics are highly complex in any interconnected systems, and often the resultant damping ratio of oscillations are unknown due to the large number of involved equipment [22, 23]. It is therefore challenging to identify falsely extracted information from malicious measurements, and thus making oscillation detection an attractive target to attack. Furthermore, injecting measurements to hide unstable inter-area oscillations can potentially lead to wide-area blackouts and system breakups as seen in the Northwestern blackout in the USA in 1996 [23]. Hence, oscillation detection serves as an ideal candidate example. In this paper, data-injection attacks are assumed to take place in a metering device known as Phasor Measurement Units (PMUs) installed in transmission substations. PMUs are the foundation of WAMS, where their measurements are used for WAMS applications. Comparisons have been made with Prony Analysis, which is one of the most widely adopted techniques. It was first proposed in [24] and is currently implemented in countries like Canada, USA and many other European nations [25].

In an event of an attack, the following two negative consequences can occur due to inaccurate monitoring and time complexity of the algorithms. 1) If the data is altered in a way that is not detectable as false dynamics by monitoring schemes, the perceived observable state of the system will be wrong. This will then lead to improper control actions, which may endanger the security of the system. 2) The malicious intent might not be to hide the attack, but to force part of the system to become unobservable due to the collective behavior among the network of nodes. This can blind the system operators and increase the vulnerability of the grid to further attacks or inappropriate operations. More importantly, regardless to any consequences, the impacts of acting on incorrect or missing information will have already propagated into the rest of the system. At this stage, it may already be too late to avoid a wide-area power outage within the grid.

Therefore, this paper proposes a way to minimize the potential damages of multiple data-injection attacks through novel processing of information collected from a set of distributed PMU sensors. A recursive Bayesian filter-based solution is formulated to enhance the observability of monitoring methods with resilience against contaminated measurements. This approach does not require additional physical upgrades of existing PMU sensors, which minimize the necessary investments for utilities. The proposed Bayesian filter-based method also utilized the architecture of the latest distributed oscillation detection method proposed in [26]. This is due to its recent breakthrough on a recursive platform [27, 28].

An overview of the proposed methodology is shown in Fig. 1. It summarizes the formulations and equations involved at each step. The considered scenario assumes an attacker is smart enough to inject data that imitates regular variations of small-signal system dynamics in the electrical grids. In the context of the presented example application, the perceived aim is to generate or hide lightly damped inter-area oscillations. Moreover, the possibility of adding a bias to cancel the critical information from some monitoring nodes has been studied. In this paper, a monitoring node refers to a site where Bayesian-based approximated filter (BAF) is applied to extract oscillation parameters from PMU measurements. It begins by developing the measurement models, which involve the dynamical and observation models, followed by the state representation of electromechanical oscillations. The proposed scheme is further enhanced based on characterizing the unobservable attack using the Bayesian inference, which determines the relative loss of information. This concern is further tackled by BAF by manipulating estimated oscillation parameters from all monitoring nodes. This is done by generating the attack vectors and a rank matrix for fault injection detection. The properties of the rank matrix are highly dependent on the amount of information loss due to the attack. Furthermore, upper and lower bounds have also been developed to reduce the computing time. The distributed fusion center

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2544854, IEEE Transactions on Smart Grid

(DFC) is then developed to compute and minimize the errors of filtering and estimation within each monitoring node. This results to improving the monitoring accuracy of oscillatory frequencies.

Notations: In this paper, **E** is the expectation operator. A symbol $\hat{\cdot}$ over a variable indicates an estimate of that variable e.g. $\hat{x}$ is an estimate of x. A symbol * is a transpose operator. The individual entries of a variable like x are denoted by $x(l)$. When any of these variables become a function of time, the time index t appears as a subscript e.g. x_t. When any of these variables are collected from a node i or j, it will appear also as a part of superscript e.g. x_t^i, x_t^j. The notation x_0^T is used to denote the time sequence e.g. x_0, x_1, ..., x_T. Similarly, $\overline{x}$ denotes the upper bound and $\underline{x}$ denotes the lower bound respectively.

II. Distributed Monitoring of a Power Grid in the Presence of Severe Data-Injection

Consider a power grid having multiple buses, where each bus is monitored by a PMU that is proned to data-injection attacks. Note a PMU installed site is also referred as a node, and all PMUs operate at the same sampling rate. It has been initially assumed that there is no information loss between the PMU nodes. Additionally, perturbations and random fluctuations are part of noise-induced transitions. As a result, a general discrete-time dynamic model of i-th node can be represented as:

$$x_{t+1}^i = \sum_{j=1}^{N} F_t^{ij} x_t^j + G_t^i w_t^i,\ t = 0,1,2,....T \tag{1}$$

where $x_t \in \mathbf{R}^r$ is the state variable at the i-th node, superscript r is the size of the state vector in the subspace $\mathbf{R}$. $F_t \in \mathbf{R}^{r\times r}$ is a model matrix of the state response from i-th node to j-th node for $i \neq j$. $F_t^{ij} x_t^j$ is a control input from the node i to the node j for $i \neq j$. Meanwhile, $G_t^i \in \mathbf{R}^{r\times r}$ is the noise transition matrix, which can be defined as the probability vector whose elements are the non-negative real numbers and sum to 1. $w_t^i \in \mathbf{R}^r$ is the random process noise, t is the time-instant, and T refers to the number of time-instants. In this context, PMU nodes do share the information between themselves over a communication network such that a packet of information sent by the i-th node is correctly received by the j-th node with a probability p_{ij}. Suppose χ_t^{ij} be a Bernoulli random variable representing such situation. This can be defined as $\chi_t^{ij} \in \{0,1\}$, such that $\chi_t^{ij} = 1$, if the packet of information sent by i-th node is correctly received by j-th node at t-th instant. Similarly, $\chi_t^{ij} = 0$ if the pack of information at i-th node is not received at j-th node. Thus, the general dynamic model in (1) can be further represented as:

$$x_{t+1}^i = \sum_{j=1}^{N} \chi_t^{ij} F_t^{ij} x_t^j + G_t^i w_t^i \tag{2}$$

However, the state variable at i-th node shall be an explicit representation of discrete-time variant while involving the interaction between i-th and j-th nodes. To determine the represenation, let $x_t^i = [x_t^{1^*}, ..., x_t^{N^*}]$ and $w_t^i = [w_t^{1^*}, ..., w_t^{N^*}]$ while G_t^i be a block diagonal matrix of $G_t^1, ..., G_t^N$ that represents the transition of the random process noise. Note that $\bar{F}_t^{ij}$ is an $\mathbf{R}^{r\times r}$ block matrix, where its entries are all zero except for the (ji)-th element of which contains the interaction between i-th and j-th nodes. Then (2) can be represented for an explicit discrete-time representation of x_{t+1}^i as $(\sum_{i=1}^{N}\sum_{j=1}^{N} \chi_t^{ij}\bar{F}_t^{ij})x_t^i + G_t^i w_t^i$. Let $ij = N(i-1)+j$, then, the dynamical model in (1) can be rewritten as $x_{t+1}^i = (\sum_{ij=1}^{N^2} \chi_t^{ij}\bar{F}_t^{ij})x_t^i + G_t^i w_t^i$. It should be noted that the model matrix of the state response $\bar{F}^{ij}$ is time-varying, where its values are determined by the probability of Bernoulli's random variable χ_t^{ij}. Hence, χ^{ij} can be considered as a function of $\bar{F}^{ij}$, and x_{t+1}^i can now account for the random system perturbations as:

$$x_{t+1}^i = \chi^{ij}(\bar{F}_t^{ij})x_t^i + G_t^i w_t^i \tag{3}$$

Now, suppose the power grid described in (3) is monitored by collecting information from N number of PMU nodes in a distributed environment. Furthermore, parametric computation is conducted at a central station, i.e. a distributed fusion center (DFC), which involves information from each local node and estimated sequences are generated in the presence of random noise fluctuations. The observations vector for extracting the states at the i-th node possibly affected by the attack can be defined as:

$$z_t^i = h_t^i(x_t) + \upsilon_t^i,\ i = 1, ..., N \tag{4}$$

where $z_t^i \in \mathbf{R}^{p^i}$, p^i is the number of synchrophasor observations made by the i-th PMU, $h^i(.)$ is a nonlinear function representing the local observation matrix of i-th PMU, x_t is the state matrix containing the system parameters, and $\upsilon_t^i \in \mathbf{R}^{p^i}$ is the observation noise of the i-th PMU. Note that the noises w_t and ν_t are all initially assumed to be uncorrelated zero-mean white Gaussian.

Once the observation model is constructed from collected synchrophasor measurements, the corresponding state representation of the desired application can be formulated in the frequency domain. As discussed in the introduction, the application example used in this paper is the oscillation detection. Its problem formulation will be presented in the next section, followed by the mathematical development of the Bayesian-based immunity scheme.

A. Electromechanical Oscillation Model Formulation

Suppose a measured noise-induced signal containing K number of electromechanical oscillations. Referring to (4), the observation output signal z_t^i from an i-th PMU at time t can be modeled in the frequency domain as:

$$z_t^i = \sum_{k=1}^{K} a_k e^{(-\sigma_k + j2\pi f_k)tT_s} + \upsilon_t^i,\ t = 1,2,....., T \tag{5}$$

where a_k is the complex amplitude of k-th mode, σ_k is the damping factor, f_k is the oscillatory frequency, and T_s is the sampling time [26]. For convenience, the term $-\sigma_k + j2\pi f_k$ is represented in the rectangular form as λ_k. In this paper, the k-th oscillation or eigenvalue within a mentioned signal is described by two states denoted as $x_{k,t}$ and $x_{k+1,t}$, respectively. They can also be expressed in the context of an i-th PMU as:

$$x_{k,t}^i = e^{(-\sigma_k + j2\pi f_k)tT_s},\ x_{k+1,t}^i = b_{k+1}e^{(-\sigma_{k+1} + j2\pi f_{k+1})tT_s} \tag{6}$$

The term b_k represents the complex amplitude of the k-th mode. The damping factor σ_k and the corresponding frequency f_k of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2544854, IEEE Transactions on Smart Grid

each oscillation can be computed from the state x_t. Estimating oscillatory parameters for an accurate WAMS will require the complete observability of the observation matrix. This is quiet challenging in the presence of data-injection attacks. Locational awareness for each node is required, considering the fact that installed PMUs may also malfunction during an attack. Considering imperfect PMU measurements, a statistical tool is required to handle the situations of uncertainty during power system operations. The property of Bayesian filter to probabilistically estimate a dynamic system prone to data-injection attacks is presented here. Moreover, its abstract concept to provide probabilistic framework for recursive estimation in the presence of high noise or uncertainty will assist in achieving a more accurate WAMS. The derived Bayes filter is proposed to provide inferences that are conditional on the health of the measurements without reliance on asymptotic approximations.

B. Characterization of Attack using Bayesian Inference

An initial characterization about the unobservable attacks can be made by Bayesian inference. Assume the probabilities on *a-prior* distribution over the oscillatory states at i-th node are $p(x_t^i)$, and the observation matrix is $p(H_t^i|x_t^i)$. The resultant posterior distribution over the observations can be represented by the Bayesian inference as:

$$p(x_t^i|z_t^i) = \frac{p(x_t^i)p(z_t^i|x_t^i)}{p(z_t^i)} \tag{7}$$

To quantify the uncertainty of possible data-injection attacks, the density of the predicted synchrophasor observations is required to be computed. This can be obtained by averaging over the uncertainty of data-injection attacks on the oscillatory states and the observation matrix. Let $z_{pr,t}^i$ represent the predicted synchrophasor observations at i-th node, then $z_{pr,t}^i$ can be presented in the form of predictive distribution as:

$$p(z_{pr,t}^i|z_t^i)=\sum_{x_t^i}\int dH_t^i p(z_{pr}^i|H_t^i,x_t^i,z_t^i)p(H_t^i|x_t^i,z_t^i)p(x_t^i|z_t^i) \tag{8}$$

where the posterior distribution about the data-injection attack is learnt by the predicted synchrophasor observations. This distribution will further assist in the development of the probability of the attack vectors and the identification of the parameters as well as the natural noise manipulation. In general, the natural system noise and its colors have a constant or integral power spectral density with a sequence of serially uncorrelated random variables. Having said that, once a new unseen synchrophasor observation comes in at time-instant $t+1$, the distribution over the possible predicted synchrophasor observations is calculated given the learnt posterior distribution about the data-injection attacks. This fact will be further verified by the scheme in the later stage by assuming the unobservability in the measurements. Such an assumption will direct towards estimating the latency and noise distribution of the local nodes. When all the information are gathered at the distribution fusion center, the method can then detect critical variations in the noise of any local nodes. As a result, the difference between the signature of the natural system noise and the attack manipulation can be determined accordingly. Note that the attacks on the neighboring nodes have no impact on such detection approach.

C. Detecting Data-Injection using Initial Observation Analysis

Once the probability of attack vectors is developed, the attack can be detected by doing an initial observation analysis of the measurements using the calculation of gradient between the measurements. This can be achieved by taking the difference between the given and predicted observation of the oscillation state:

$$\mathcal{Z}_{t+1}^i = [z_{t+1}^i - z_{pr,t+1}^i] = \sum_{t=1}^{T}\psi_{t-1}^*\theta_t^i\Delta H_t^i + \nu_t^i \tag{9}$$

where the vector $\mathcal{Z}_{t+1}^i$ is the innovation calculated for i-th node. z_{t+1}^i and $z_{pr,t+1}^i$ are the data-injection free (nominal) and predicted affected observation outputs, respectively. $\Delta H_t^i = H_{d,t}^i - H_t^i$ is the perturbation in H_t^i. $\theta_t^i = \frac{\delta z_t^i}{\delta H_t^{i*}}$ is the gradient used to identify the perturbation due to data-injection attacks. ψ_t is the data vector formed from past outputs and reference inputs at each node.

Once, the PMU nodes affected by the data-injection attacks have been characterized, a Bayesian filter with an assumption of no prior information can be derived.

D. Bayesian Filter with no Prior Information

Consider the worst case scenario of information loss to be very high. This means there is no regular prior information about the oscillatory states. The possibility can be either the prior covariance is not known or information does not exist due to the impact of an attack. Therefore, the calculation of innovation for the state prediction will not involve the *a-prior* knowledge. Considering (4) with known $\bar{\nu}_t^i = \mathbf{E}[\nu_t^i]$ at i-th node, an oscillation state prediction $\hat{x}_{t+1|t}^i$ exists if and only if the observation matrix H_t^i has a full column-rank, or equivalently $det(H_t^{i^*}H_t^i) \neq 0$. Since there is no prior knowledge of involved states, the resulting state-prediction will be:

$$\begin{aligned}\hat{x}_{t+1|t}^i &= \mathbf{E}[x_{t+1}^i e_t^{i^*}]R_{e,t}^{i^{-1}}e_t^i \\ &= \mathbf{E}[x_{t+1}^i e_t^{i^*}]R_{e,t}^{i^{-1}}(z_t^i - \nu_t^i)\end{aligned} \tag{10}$$

where $\nu_t^i \perp z_t^i$, $(\mathbf{E}x_{t+1}e_t^*)R_{e,t}^{-1}$ can be defined as a predicted gain matrix denoted by $K_{pr,t}^i$, where the subscript pr indicates that $K_{pr,t}^i$ is used to update the predicted oscillation state at i-th node. $R_{e,t}$ is the covariance of noise. The estimated state can then be expressed as:

$$\hat{x}_{t|t}^i = K_{pr,t}^i[z_t^i - \nu_t^i] \tag{11}$$

From (3), $F_{pr,i}^i$ for prediction can be stated as $F_t^i - K_{pr,t}^i H_t^i$. Thus (10) becomes:

$$\begin{aligned}\hat{x}_{t+1|t}^i&=(F_t^i - K_{p,t}^i H_t^i)\hat{x}_{t|t-1}^i + K_{p,t}^i(z_t^i - \nu_t^i) \\ &=F_t^i\hat{x}_{t|t-1}^i - K_{pr,t}^i H_t^i\hat{x}_{t|t-1}^i + K_{pr,t}^i z_t^i - K_{pr,t}^i\nu_t^i\end{aligned} \tag{12}$$

Since at i-th node,

$$\begin{aligned}K_{pr,t}^i &= \mathbf{E}[x_{t+1}e_t^*]R_{e,t}^{i^{-1}} \\ &= \mathbf{E}[(\chi^{ij}(F_t^{ij})x_t^i + G_t^i w_t^i)e_t^*]R_{e,t}^{i^{-1}}\end{aligned} \tag{13}$$

Given $\tilde{x}_{t|t-1}^i = x_{t+1}^i - \hat{x}_{t|t-1}^i$, it can rearrange into $x_{t+1}^i = \hat{x}_{t|t-1}^i + \tilde{x}_{t|t-1}^i$ and make $\mathbf{E}[x_t^i e_t^{i^*}]$ becomes:

$$\mathbf{E}[x_t^i e_t^{i^*}] = \mathbf{E}[\tilde{x}_{t|t-1}^i e_t^{i^*}] \tag{14}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2544854, IEEE Transactions on Smart Grid

Knowing $e_t^i \perp \hat{x}_{t|t-1}^i$, thus,

$$\begin{aligned}\mathbf{E}[x_t^i e_t^{i^*}] &= \mathbf{E}[\tilde{x}_{t|t-1}^i (H_t^i \tilde{x}_{t|t-1}^i + \nu_t^i)] \\ &= \mathbf{E}[\tilde{x}_{t|t-1}^i (H_t^i \tilde{x}_{t|t-1}^i + 0)] \end{aligned} \quad (15)$$

Also $\nu_t^i \perp \tilde{x}_{t|t-1}^i$, which shows,

$$\mathbf{E}[x_t^i e_t^{i^*}] = P_{t|t-1}^i H_t^{i^*} \quad (16)$$

From (13), $\mathbf{E}[w_t^i e_t^{i^*}]$ can be calculated as:

$$\mathbf{E}[w_t^i e_t^{i^*}] = \mathbf{E}[w_t^i (H_t^i \tilde{x}_{t|t-1}^i + \nu_t^i)^*] \quad (17)$$

Since $w_t^i \perp \tilde{x}_{t|t-1}^i$, thus,

$$\mathbf{E}[w_t^i e_t^{i^*}] = 0 + \mathbf{E}[w_t^i \nu_t^{i^*}] = S_t^i \quad (18)$$

Therefore, (13) becomes,

$$\begin{aligned} K_{pr,t}^i &= \mathbf{E}[x_{t+1}^i, e_t^{i^*}] R_{e,t}^{i^{-1}} \\ &= (\chi^{ij}(F_t^{ij}) P_{t|t-1}^i H_t^{i^*} + G_t^i S_t^i) R_{e,t}^{-1} \\ &= [cov(x_t^i) H_t^{i^*} + cov(x_t^i, \nu_t^i)] cov(y_t^i)^{-1} \end{aligned} \quad (19)$$

In case of no *a-priori* information, oscillatory states x_t^i exists if and only if H_t^i has full column rank such that $H_t^{i^+} = (H_t^{i^*} H_t^i)^{-1} H_t^{i^*}$, where superscript $+$ denotes the full rank. As a result, $K_{pr,t}^i$ becomes:

$$\begin{aligned} &= H_t^{i^+} [I - \chi^{ij}(F_t^{ij}) P_{t|t-1}^i (I - H_t^i H_t^{i^*}) \chi^{ij}(F_t^{ij}) P_{t|t-1}^i (I \\ &\quad - H_t^i H_t^{i^*})^+] \end{aligned} \quad (20)$$

In addition, the gain matrix could prove to be very vulnerable in the presence of no *a-priori* information. Therefore, an optimal gain $\tilde{K}_t^i$ at i-th node is required to be generated to ensure stability of the system by considering this a quadratic optimization problem, which gives (20) as $K_{pr,t}^i = \arg\min_{H_t^{i^+} K_{pr,t}} (K_t^* \chi^{ij}(F_t^{ij}) P_{t|t-1}^i K_t^*)$. Using the generalized inverse theory in [29], (20) can be represented in the form of optimal gain $\tilde{K}_t^i$ as:

$$\begin{aligned} \tilde{K}_t^i &= [I - (I - H_t^i H_t^{i^*}) \chi^{ij}(F_t^{ij}) P_{t|t-1}^i (I - H_t^i H_t^{i^*})^+ \\ &\quad \chi^{ij}(F_t^{ij}) P_{t|t-1}^i] \\ &\quad (H_t^+)^* + (I - H_t^i H_t^{i^*}) B_t^i \\ \tilde{K}_t^i &= K_t^i + (I - H_t^i H_t^{i^*}) B_t^i \end{aligned} \quad (21)$$

where B_t^i is any matrix of compatible dimensions satisfying $P_{t|t-1}^{1/2^{i^*}} (I - H_t^i H_t^{i^*}) B_t^i = 0$, $P_{t|t-1}^{i^{1/2}}$ is any square-root matrix of $P_{t|t-1}^i$. The optimal gain matrix $\tilde{K}_t^i$ is given uniquely by:

$$\begin{aligned} \tilde{K}_t^i = H_t^{i^+} [I - \chi^{ij}(F_t^{ij}) P_{t|t-1}^i (I - H_t^i H_t^{i^+})^{1/2} (I - H_t^i H_t^{i^+})^{1/2^*} \\ \chi^{ij}(F_t^{ij}) P_{t|t-1}^i (I - H_t^i H_t^{i^{+1/2}})^{-1} (I - H_t^i H_t^{i^+})^{1/2^*}] \end{aligned} \quad (22)$$

The optimal gain matrix is true if and only if $[H_t^i, P_{t|t-1}^{i^{1/2}}]$ has full row-rank, where $(I - H_t^i H_t^{i^+})^{1/2}$ is a full-rank square root of $(I - H_t^i H_t^{i^*})$. This is due to the information collected from each node.

Once the optimal gain is calculated, the covariance matrix to calculate the error of estimation is required for i-th node. Let P_t^i denote the covariance matrix of x_t^i, such that $\mathbf{E}[(x_{t|t-1}^i - \hat{x}_{t|t-1}^i)(x_{t|t-1}^i - \hat{x}_{t|t-1}^i)^*]$. Since, $e_t^i \perp \hat{x}_{t|t-1}^i$, it can be seen that $\hat{x}_{t+1|t}^i = F_t^i \hat{x}_{t|t-1}^i - K_{pr,t}^i H_t^i x_{t+1|t}^i + K_t^i z_t^i - K_t^i \nu_t^i$. The covariance matrix of $\hat{x}_{t|t-1}^i$ should satisfy the recursion with no *a-priori* information as $\nu_t^i = \mathbf{E}\hat{x}_{t|t-1}^i \hat{x}_{t|t-1}^{i^*}$. This gives covariance matrix to be:

$$P_{t+1}^i = cov(x_t^i) - K_t^i cov(z_t^i) K_t^{i^*} \quad (23)$$

Since there is no *a-priori* information and orthogonal decomposition of x_t^i has $\hat{x}_{t|t-1}^i \perp x_t^i - \hat{x}_{t|t-1}^i$, the estimated covariance matrix $P_{t+1|t}^i$ is the difference between covariance matrix of x_t^i, Υ_{t+1}^i and $\hat{x}_{t|t-1}^i$, Π_{t+1}^i. Since, there is no *a-priori* information, therefore,

$$\begin{aligned} P_{t|t-1}^i &= \Upsilon_{t+1}^i - \Pi_{t+1}^i \\ &= 0 + K_{pr,t}^i R_{e,t}^i K_{pr,t}^{i^*} \\ &= K_{pr,t}^i R_{e,t}^i K_{pr,t}^{i^*} \end{aligned} \quad (24)$$

Thus, the parameters like estimated states, predicted gain matrix, optimal gain, and covariance matrix of Bayesian filter with probability of no *a-priori* information are derived. Note the proposed scheme can also be applied to other dynamic monitoring applications using PMU measurements. The user can simply replace the problem formulation of Section II-A with the desired one. Subsequent formulation of the Bayesian filter will be the same.

E. Modified Filter with no a-priori Information

Based on the power grid model expressed in (3), an optimal filter is derived given χ^{ij} is a function of the transition state F_t^{ij}. Let $\hat{x}_{t|t}^i$ and $P_{t|t}^i$ be the estimated states and covariance matrix at time-instant t. To calculate measurement at time-instant $t+1$, a measurement z_{t+1}^i is received to estimate $\hat{x}_{t+1|t}^i$ from $\hat{x}_{t|t}^i$, and $P_{t+1|t}^i$ from $P_{t|t}^i$ respectively. $\hat{x}_{t+1|t}^i$ will be computed as:

$$\begin{aligned} \hat{x}_{t+1|t}^i &= \mathbf{E}[x_{t+1}^i | z_t^i] \\ &= \mathbf{E}[\chi^{ij}(F_t^{ij}) x_t^i + G_t^i w_t^i | z_t^i] = \hat{\chi}_F^{ij} \hat{x}_{t|t}^i \end{aligned} \quad (25)$$

where $\hat{\chi}_{F,t}^{ij}$ is the expected value of $\chi^{ij}(F_t^{ij})$, such that $\hat{\chi}_{F,t}^{ij} = \sum_{F_t \in \mathbf{R}} p_{F^{ij}}[\chi^{ij}(F_t^{ij})]$. The prediction covariance can be computed for an i-th PMU as:

$$\begin{aligned} P_{t+1|t}^i = \mathbf{E}[e_{t+1|t}^i e_{t+1|t}^{i^*} | z_t^i] = -K_{pr,t}^i R_{e,t}^i K_{p,t}^{i^*} \\ + \sum_{F_t \in R} p_{F^{ij}}[\chi^{ij}(F_t^{ij}) \hat{x}_{t|t}^{i^*}] (\chi^{ij}(F_t^{ij}) - \hat{\chi}_{F,t}^{ij}) \end{aligned} \quad (26)$$

Given $\hat{x}_{t+1|t}^i$ and $P_{t+1|t}^i$, the updated a-posteriori estimate $\hat{x}_{t+1|t+1}$ and $P_{t+1|t+1}$ are computed similar to the standard Kalman filter:

$$\begin{aligned} \hat{x}_{t+1|t+1}^i &= K_{t+1}^i [z_{t+1}^i - \nu_t^i] \\ P_{t+1|t+1}^i &= K_{t+1}^i H_{t+1}^i P_{t+1}^i \end{aligned} \quad (27)$$

where $K_{t+1}^i = H_{t+1}^{i^+} [I - P_{t+1}^i (I - H_t^i H_t^{i^*}) P_{t+1}^i]$.

F. Reducing the Time Complexity using Approximate Filter

The modified filter proposed for the power grid expressed in (3) is an optimal filter. However, if data-injection attack occurs frequently in nodes, the time complexity of the modified filter

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2544854, IEEE Transactions on Smart Grid

can be exponential in N since the size of the state transition matrix F_t^{ij} is $O(2^{N(N-1)})$ in the worst case, when all the nodes suffered with data-injection attacks. There is a need to approximate the filter to reduce the computational load on the system. As a result, two bounds have been introduced for the power grid model in (3) to avoid the enumeration on F_t^{ij}. Since the computation of $P^i_{t+1|t}$ is the only time consuming process, bounds have been introduced into $P^i_{t+1|t}$, which are generated from i-th monitoring node. Note the notation $\chi^{ij}_{F,t} \geq 0$ is used if $\chi^{ij}_{F,t}$ is a positive semi-definite matrix, and $\chi^{ij}_{F,t} \geq 0$ if $\chi^{ij}_{F,t}$ is a positive definite matrix.

1) Lower Bound for Reducing Time Complexity: As the bounds are applied on the covariance matrix collected from each node, $P^i_{t+1|t}$ would be approximated by $\underline{P}^i_{t+1|t}$ and $P^i_{t|t}$ would be approximated by $\underline{P}^i_{t|t}$ at i-th PMU respectively. The covariances are updated as:

$$\underline{P}^i_{t+1|k} = \underline{K}^i_{t+1} R^i_t \underline{K}^{i^*}_{t+1} \tag{28}$$

$$\underline{P}^i_{t+1|t+1} = \underline{K}^i_{t+1} H^i_t \underline{P}^{i^*}_{t+1|t} \tag{29}$$

where $\underline{K}^i_{t+1} = H^{i^+}_t [I - \underline{P}^i_{t+1|t}(I - H^i_t H^{i^*}_t)\underline{P}^i_{t+1|t}]$.

However, the conditions of semi-positiveness should be ensured for feasibility of the lower bound, which says that:

- *Condition 1:* If $\underline{P}^i_{t|t} \leq P^i_{t|t}$, then $\underline{P}^i_{t+1|t} \leq P^i_{t+1|t}$.
- *Condition 2:* If $\underline{P}^i_{t+1|t} \leq P^i_{t+1|t}$, then $\underline{P}^i_{t+1|t+1} \leq P^i_{t+1|t+1}$.

In the case of *Condition 1* expressed at i-th PMU, the prediction covariance matrix in (26) becomes:

$$\begin{aligned} P^i_{t+1|t} - \underline{P}^i_{t+1|t} &= E[\chi^{ij}(F^{ij}_t)\hat{x}^i_{t|t}\hat{x}^{i^*}_{t|t}\chi^{ij}(F^{ij}_t)^*] - K^i_{pr,t}R^i_{e,t}K^{i^*}_{pr,t} \\ &\quad - \hat{\chi}^{ij}\hat{x}^i_{t|t}\hat{x}^{i^*}_{t|t}\hat{\chi}^{ij^*} - \underline{K}^i_{pr,t}\underline{R}^i_{e,t}\underline{K}^{i^*}_{p,t} \\ &= P^i_{1,t} + P^i_{2,t} \end{aligned} \tag{30}$$

where,

$$P^i_{1,t} = K^i_{pr,t}R^i_{e,t}K^{i^*}_{pr,t}, \text{and} \tag{31}$$

$$\begin{aligned} P^i_{2,t} &= \mathbf{E}[\chi^{ij}(F^{ij}_t)\hat{x}^i_{t|t}\hat{x}^{i^*}_{t|t}\chi^{ij}(F^{ij}_t)^*] - \hat{\chi}^{ij}\hat{x}^i_{t|t}\hat{x}^{i^*}_{t|t}\hat{\chi}^{ij^*} \\ &\quad - \underline{K}^i_{pr,t}\underline{R}^i_{e,t}\underline{K}^{i^*}_{pr,t}. \end{aligned} \tag{32}$$

Since $P^i_{t|t}$ is a symmetric matrix, it can be decomposed into $P^i_{t|t} = U^i_{1,t}D^i_{1,t}U^{i^*}_{1,t}$, where $U^i_{1,t}$ is a unitary matrix and $D^i_{1,t}$ is a diagonal matrix at i-th node. As there is no $P^i_{t|t}$ for $P^i_{1,t}$ here, $P^i_{1,t} = -K^i_{pr,t}R^i_{e,t}K^{i^*}_{pr,t}$.

For *Condition 2*, matrix inversion lemma can be used, which defines that $(A^i_t + U^i_t C^i_t V^i_t)^{-1} = A^{i^{-1}}_t - A^{i^{-1}}_t U^i_t (C^{i^{-1}}_t + V^i_t A^{i^{-1}}_t U^i_t)^{-1} V^i_t A^{i^{-1}}_t$ where A^i_t, U^i_t, C^i_t and V^i_t are the matrices of correct size at i-th node. Applying the matrix inversion lemma to (27), it gives $P^i_{t+1|t+1} = (P^{i^{-1}}_{t+1|t} + H^{i^*}_t R^{i^{-1}}_{e,t} H^i_t)^{-1}$. Let $P^i_t = P^i_{t+1|t}$ and $\underline{P}^i_t = \underline{P}^i_{t+1|t}$. Then $P^i_t \geq \underline{P}^i_t$, $P^{i^{-1}}_t \leq \underline{P}^{i^{-1}}_t$. Also, $P^{i^{-1}}_t + H^{i^*}_t R^{i^{-1}}_{e,t} H^i_t \leq \underline{P}^{i^{-1}}_t + H^{i^*}_t R^{i^{-1}}_{e,t} H^i_t$, $(P^{i^{-1}}_t + H^{i^*}_t R^{i^{-1}}_{e,t} H^i_t)^{-1} \geq (\underline{P}^{i^{-1}}_t + H^{i^*}_t R^{i^{-1}}_{e,t} H^i_t)^{-1}$. This gives $P^i_{t+1|t+1} \geq \underline{P}^i_{t+1|t+1}$.

The feasibility of *Condition 1* and *Condition 2* is generated to prove that the state error covariance is maintained by the lower-bound of the modified filter. To further elaborate, let $\underline{P}^i_{0|0}$ denotes the initial covariance on lower bound, such that $\underline{P}^i_{0|0} \geq P^i_{0|0}$, then $\underline{P}^i_{t|t} \geq P^i_{t|t}$ for all $t \geq 0$.

2) Upper Bound for Reducing Time-Complexity: Similar to the lower bound, the upper-bound has been applied on the covariance matrix to reduce time-complexity. $\overline{P}^i_{t+1|t}$ approximates $P^i_{t+1|t}$ and $\overline{P}^i_{t|t}$ approximates $P^i_{t|t}$. Let $\lambda_{max} = \lambda_{max}(\overline{P}^i_{t|t} + \lambda_{max}(\hat{x}^i_{t|t}\hat{x}^{i^*}_{t|t})$, where λ_{max} represents the maximum eigenvalue. The covariances are updated as follows:

$$\overline{P}^i_{t+1|t} = \lambda_{max}\mathbf{E}[\chi^{ij}(F^{ij}_t)\chi^{ij}(F^{ij}_t)^*] + K^i_{pr,t}R^i_{e,t}K^{i^*}_{p,t} \tag{33}$$

$$\overline{P}^i_{t+1|t+1} = \overline{K}^i_{t+1} H^i_t \overline{P}^i_{t+1|t} \tag{34}$$

where $\overline{K}^i_{t+1} = H^{i^+}_t [I - \overline{P}^i_{t+1|t}(I - H^i_t H^{i^*}_t)\overline{P}^i_{t+1|t}]$. In the upper bound, $\mathbf{E}[\chi^{ij}(F^{ij}_t)\chi^{ij}(F^{ij}_t)^*]$ can be computed in advance. Whereas, λ_{max} has to be computed at each step of the algorithm.

Similar to the lower bound, the feasibility condition of semi-positiveness shall be ensured for upper bound as:

- *Condition 3:* If $\overline{P}^i_{t|t} \geq P^i_{t|t}$, then $\overline{P}^i_{t+1|t} \geq P^i_{t+1|t}$.

For *Condition 3* at i-th PMU node, let $M^i_t = \hat{x}^i_{t|t}\hat{x}^{i^*}_{t|t}$ and I be an identity matrix. Then using (26),

$$\begin{aligned} \overline{P}^i_{t|t} - P^i_{t|t} &= \lambda_{max}\mathbf{E}[\chi^{ij}(F^{ij}_t)\chi^{ij}(F^{ij}_t)^*] \\ &\quad - \mathbf{E}[\chi^{ij}(F^{ij}_t)M^i_t\chi^{ij}(F^{ij}_t)^*] - \mathbf{E}[\hat{\chi}^{ij}M^i_t\hat{\chi}^{ij^*}] \\ &= \mathbf{E}[\chi^{ij}(F^{ij}_t)(\lambda_{max}I - M^i_t)\chi^{ij}(F^{ij}_t)^*] \\ &\quad + \mathbf{E}[\hat{\chi}^{ij}M^i_t\hat{\chi}^{ij^*}] + \overline{K}^i_{p,t}\overline{R}^i_{e,t}\overline{K}^{i^*}_{p,t} \\ &\quad - K^i_{p,t}R^i_{e,t}K^{i^*}_{p,t} \end{aligned} \tag{35}$$

Since $\overline{P}^i_{t|t} \geq P^i_{t|t}$ and $\lambda_{max}(Y^i_t)I - Y^i_t \geq 0$ for any symmetric matrix Y^i_t, $\overline{P}^i_{t|t} - P^i_{t|t} \geq 0$.

The feasibility of *Condition 3* generates to prove that the upper bound maintains the oscillation state error covariance of the modified filter. If the upper bound starts with an initial covariance $\overline{P}^i_{0|0}$, such that $\overline{P}^i_{0|0} \geq P^i_{0|0}$, then $\overline{P}^i_{t|t} \geq P^i_{t|t}$ for all $t \geq 0$.

3) Convergence: Theorem II.1 shows a simple condition when the oscillation state error covariance is unbounded.

Theorem II.1: If $(E[\chi^{ij}(F^{ij}_t)]^*, E[\chi^{ij}(F^{ij}_t)]^* H^{i^*}_t)$ is not stabilizable, or equivalently, $(E[\chi^{ij}(F^{ij}_t)], H^i_t E[\chi^{ij}(F^{ij}_t)])$ is not detectable, then there exists an initial covariance $P^i_{0|0}$ such that $P^i_{t|t}$ diverges as $t \to \infty$.

Proof: This is proved in the Appendix. ■

G. Distributed Fusion Center (DFC)

Once all the information about the covariance and estimated states are collected from local PMU nodes, they will be treated at the DFC. Its purpose is to improve the accuracy of the covariance and estimated states in the presence of data-injection attacks. Similar to (4), the corresponding observation model and noise vector for DFC is H^{DFC}_t, and w^{DFC}_t respectively. Alternatively, they can be expressed as an array of information collected from all the PMU nodes, such that $z^{\text{DFC}}_t = [z^1_t, ...z^N_t]^*$, $H^{\text{DFC}}_t = [H^1_t, ...H^N_t]^*$, and $w^{\text{DFC}}_t = [w^1_t, ...w^N_t]^*$. Recall that N is the number of sensors. Considering the DFC-based estimation variables z^{DFC}_t, H^{DFC}_t, and w^{DFC}_t, the estimated states at

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2544854, IEEE Transactions on Smart Grid

DFC can be formulated as:

$$\hat{x}^{\text{DFC}}_{t|t} = P^{\text{DFC}}_{t|t} \sum_{i=1}^{N} P^{i^{-1}}_{t|t} \hat{x}^{i}_{t|t} \tag{36}$$

where $P^{\text{DFC}}_{t|t} = [\sum_{i=1}^{N} P^{i^{-1}}_{t|t}]^{-1}$. Moreover, considering the interactions between local nodes, the covariance matrix for i-th and j-th nodes is:

$$P^{ij}_{t|t} = \mathbf{E}[\tilde{x}^{i}_{t|t} \tilde{x}^{j^{*}}_{t|t}] = [1 - w^{i}_{t} H^{i}_{t}] P^{ij}_{t|t-1} [1 - w^{j}_{t} H^{j}_{t}]^{*} \tag{37}$$

where $\tilde{x}_{t|t} = x_{t|t} - \hat{x}_{t|t}$.

Once the formulation has been defined, the pseudo code is represented for the implementation.

H. Summary of Pseudo Code Representation:

The presented method can also be transformed into a pseudo code as seen in Algorithm 1. The variables used in the code are defined from Line 1 to 13. This is followed by the extraction of model from the PMU measurements at each i-th location. A *for loop* is applied to calculate the information about the model information, electromechanical oscillations, developing attack vectors, data injection detection, and the Bayesian-based approximation filter from each location. These loops can be seen in Line 14 to 17, 18 to 20, 21 to 23, and 24 to 27 respectively. Once the information is collected from each PMU, a *for loop* for the distributed fusion center is applied to compute all the local measurements. This requires a cumulative *for loop* as shown in Line 28 to 31. The final model extraction takes place in Line 32–33, where results about the estimated eigenvalues, oscillatory frequencies, and damping factors are then calculated.

Algorithm 1 Pseudo code of the proposed schemes

1: $N \rightarrow$ number of substations,
2: $MI \rightarrow$ model information,
3: $PMU \rightarrow$ phasor measurement unit,
4: $EO \rightarrow$ electromechanical oscillations,
5: $CUA \rightarrow$ characterizing unobservable attacks,
6: $DAV \rightarrow$ developing attack vectors,
7: $DID \rightarrow$ data injection detection,
8: $BAF \rightarrow$ Bayesian-based approximated filter,
9: $LB \rightarrow$ lower bound,
10: $UB \rightarrow$ upper bound,
11: $OF \rightarrow$ oscillation frequency,
12: $DR \rightarrow$ damping ratio,
13: $DFC \rightarrow$ distributed fusion center,
14: **for** i=1 to N+1 //including DFC
15: $\boldsymbol{MI}_i \leftarrow$PMUmeasurements($\boldsymbol{N}_i$);
16: $\boldsymbol{EO}_i \leftarrow$extract($\boldsymbol{MI}_i$);
17: **end for**
18: **for** i=1 to N
19: $\boldsymbol{DAV}_i \leftarrow$bayesianinference($\boldsymbol{CUA}_i$);
20: **end for**
21: **for** i=1 to N
22: $\boldsymbol{DID}_i \leftarrow$impactofattack($\boldsymbol{MI}_i$);
23: **end for**
24: **for** i=1 to N
25: $\boldsymbol{BAF}_i \leftarrow$timecomplexityreduction($\boldsymbol{UB}_i$);
26: $\boldsymbol{BAF}_i \leftarrow$timecomplexityreduction($\boldsymbol{LB}_i$);
27: **end for**
28: **for**j=1 to DFC
29: **for** i=1 to N
30: $\boldsymbol{MI}_{DFC} \leftarrow$update($\boldsymbol{MI}$)
31: $\boldsymbol{MI}_{DFC}$, $\boldsymbol{DAV}_{DFC}$, $\boldsymbol{DID}_{DFC}$ = localFilter($\boldsymbol{MI}_{DFC}$, $\boldsymbol{DAV}_{DFC}$, $\boldsymbol{DID}_{DFC}$);
32: **end for**
33: $\boldsymbol{eigenvalues}$, $\boldsymbol{OF}$, $\boldsymbol{DR} \leftarrow$extract($\boldsymbol{MI}$);

III. Evaluations of the Proposed Scheme

A. Test Case I: New Zealand Grid

The operation of the Bayesian-based approximation filter (BAF) is first evaluated using recorded measurements collected from the New Zealand transmission grid. The network consists of a combination of 400 kV, 220 kV, and 110 kV lines that are interconnected by HVDC links between the North and South Islands. Recorded measurements were collected from North Makarewa (NMA) and Twizel (TWZ) substations between 11:14:40 to 11:15:40 on 30 July 2008. From the recorded normal operation, the system exhibits the following electromechanical oscillations:

- Mode 1: A 0.61 Hz frequency with a 6.1% damping ratio.
- Mode 2: A 0.75 Hz frequency with a 5.6% damping ratio.

Note oscillatory parameters do not vary significantly under such ambient situation.

The aim of this test case is to validate the fundamental capability of the proposed scheme. Therefore, the implemented attacks will be limited to random and controlled data injections at North Makarewa substation. The random scenario injects white noise, whereas the controlled situation is a smarter attack making one oscillation exhibits a higher damping ratio. The intention is to mislead the operators of believing the grid is more stable, and thus delaying the supplementary damping actions. Meanwhile, the assumption is data-injection attacks intercept communication transmission or tempering the PMU with the objective to replace original measurements with manipulated values. The resultant simulated attacks are:

- First injection: A random noise attack from 11:15:00 to 11:15:05.
- Second injection: A system parameter attack to replace the damping ratio of 0.74 Hz to 8% from 11:15:20 to 11:15:28.

In this test case, Prony analysis is used as a comparative reference. It is the mainstream technique used in power oscillation detection, and has been installed in major power utilities in North America, South America, Europe, and Asia [2, 22]. However, Prony analysis was not originally formulated to consider data-injection attacks. This is due to the fundamental nature of Prony analysis, which is totally different to the proposed method. Note examining the monitoring capability during healthy conditions is not the emphasis of this study. Instead, the purpose is to gain useful insights to the potential disruptions it may suffer during data-injection attacks.

Extracted oscillatory parameters are presented in Table I. Note the results are averaged values of a 10 second time window. Referring to Table I, BAF demonstrated adequate resilience against both attacks. Its ability to manage the information loss after identifying abnormal measurements minimized the impact of an attack on extracted oscillatory parameters.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2544854, IEEE Transactions on Smart Grid

This is due to the property of designed filter, which can handle the probability densities of information even with less samples. Furthermore, MSE values are fairly consistent throughout the monitoring windows and are in the magnitude of 10^{-3}. The consistent accuracy during the first and second attack shows the injected measurements generate little threats to the reliability and security of the monitoring solutions. The recursive nature of BAF algorithm with its novelty to tackle the information loss allows it to reconstruct the original profile of the NMA as shown in Fig. 3. The initial mismatch during the second injection event was due to the recursive nature of the proposed scheme, which requires some *a-priori* information to provide the inference about the attack. This time period can be shortened if more monitoring nodes are available to provide inference from *a-priori* information of different locations.

In contrast, the estimated results of Prony analysis are less reliable. The first random attack caused incorrect estimation of both oscillations as seen in Table I. The primary advantage of Prony analysis is its ability to estimate oscillatory parameters using curve-fitting approach without prior knowledge of the system. Such merit becomes its limiting factor in the presence of an attack, where it does not have the capability to distinguish abnormal measurements. The abnormal measurements are considered as true dynamics. Hence, incorrect information will be fed to the operators as Prony analysis fits exponentially damped sinusoids to any given measurements. In this case, the false 8% damping ratio has been captured by Prony analysis and presented to the operator as seen in the 11:15:20 to 11:15:30 window. This is also the reason why Prony analysis gave reasonable MSE values despite the measurements have been subjected to data-injection attacks. Referring to Table I, MSE values are slightly higher during the attacked windows, but are not prominent enough to be considered as alarming activities. One solution can be having an additional data-processing stage like the proposed BAF to filter attacks and support the curve-fitting property of Prony analysis. Such issue is beyond the scope of this paper. Moreover, a time computation comparison has been made with the standard Kalman filter [28], BAF and implementation of upper and lower-bounds as shown in Table II. Note Kalman filter (KF) is preferred here for comparison of time computation over Prony as KF is another mainstream recursive approach similar to BAF and implementations of upper and lower bounds. Whereas Prony is a block processing technique. The results show the computation time over the entire monitoring period of 60 seconds. Comparing to the proposed BAF scheme, the upper and lower bound schemes are able to reduce the time computation by 20.91 % and 18.25 %, respectively.

B. Test Case II: Oman Electricity Network

Since power utilities only began deploying PMUs in the last decade, few grids possess large number of operational PMUs. To further evaluate the performance of the proposed scheme, a simulated transmission network of Oman has been used involving 231 Buses. The existing transmission network covers the northern Oman, and is connected with the United Arab Emirates grid. The backbone of Oman system consists of 132 kV and 220 kV lines.

TABLE I
TEST CASE I – NEW ZEALAND GRID: DETECTING OSCILLATIONS IN THE PRESENCE OF DATA-INJECTION ATTACKS

Time	**11:14:40–11:14:50**				**11:14:50–11:15:00**			
	ζ_{BAF}	f_{BAF}	ζ_{PR}	f_{PR}	ζ_{BAF}	f_{BAF}	ζ_{PR}	f_{PR}
	6.1 5.4	0.61 0.74	6.5 5.5	0.62 0.74	6.1 5.6	0.63 0.74	6.8 5.6	0.63 0.71
MSE	1.2×10^{-3}		4.2×10^{-2}		1.1×10^{-3}		4.3×10^{-2}	
Time	**11:15:00–11:15:10**				**11:15:10–11:15:20**			
	ζ_{BAF}	f_{BAF}	ζ_{PR}	f_{PR}	ζ_{BAF}	f_{BAF}	ζ_{PR}	f_{PR}
	6.1 5.6	0.62 0.74	5.4 7.1	0.65 0.72	6.1 5.6	0.63 0.75	6.8 5.7	0.63 0.75
MSE	1.7×10^{-3}		5.7×10^{-2}		1.1×10^{-3}		4.2×10^{-2}	
Time	**11:15:20–11:15:30**				**11:15:30–11:15:40**			
	ζ_{BAF}	f_{BAF}	ζ_{PR}	f_{PR}	ζ_{BAF}	f_{BAF}	ζ_{PR}	f_{PR}
	6.2 5.6	0.63 0.72	6.5 8.1	0.64 0.72	6.1 5.6	0.62 0.74	6.4 5.8	0.62 0.74
MSE	2.1×10^{-3}		7.9×10^{-1}		1.1×10^{-3}		4.1×10^{-3}	

[1]In this table, ζ is the damping ratio, f is the frequency (Hz), and MSE is the mean-square error. Subscripts BAF, and PR are the acronyms for Bayesian-based Approximated Filter and Prony Analysis, respectively.

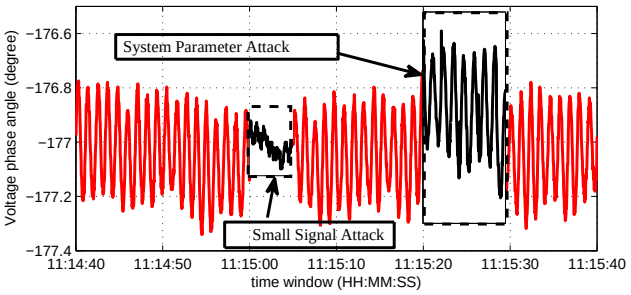

Fig. 2. Test Case I: Corrupted NMA voltage angle with data-injection attacks

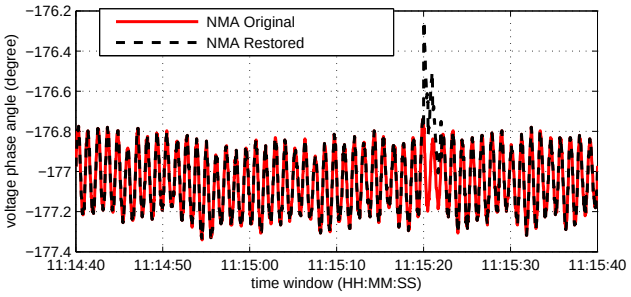

Fig. 3. Test Case I: Original and restored voltage angles of NMA node

TABLE II
TIME COMPUTATION COMPARISON FOR BOTH TEST CASES

Time	**Kalman Filter**	**BAF**	**Upper Bound**	**Lower Bound**
Test Case I	47.32	49.74	39.34	40.66
Test Case II	43.84	45.1	38.86	32.38

In this study, the network parameters are based on the projected 2015 summer peak demand scenario [31]. A total of 25 PMUs have been installed across the simulated grid. All loads are continuously being perturbed with small power fluctuations of up to 1% of their nominal values. Meanwhile, the system suffered the following disturbances over a duration of 60 seconds:

- 3-Phase Short Circuit occurred at Russail 132 kV at 5 sec-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2544854, IEEE Transactions on Smart Grid

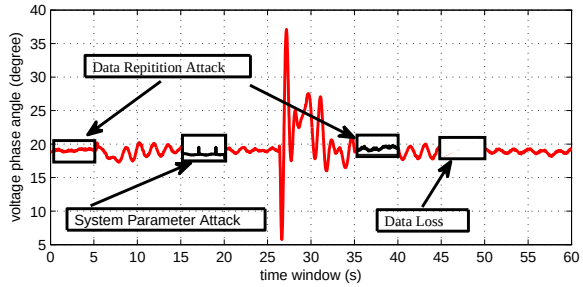

Fig. 4. Test Case II: Manipulated voltage angle at Barka substation

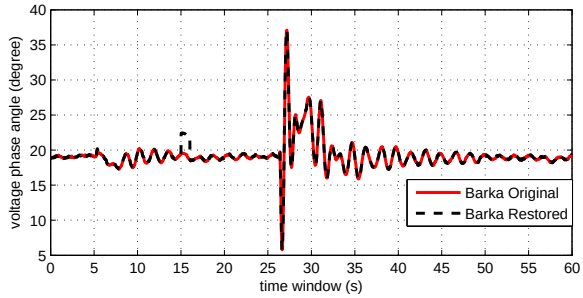

Fig. 5. Test Case II: Original and restored voltage angles of Barka node

ond and cleared at 5.1 second.

- 3-Phase short circuit event occurred at SUR IPP at 25 second and cleared after 0.1 second.

The oscillatory parameters prior to the disturbances are:

- Mode 1: A 0.64 Hz frequency with a 6.5% damping ratio.
- Mode 2: A 0.75 Hz frequency with a 5.4% damping ratio.
- Mode 3: A 0.85 Hz frequency with a 3.9% damping ratio.

On top of the system disturbances, four data-injection scenarios are included. They are:

- First injection: System parameter attack at 15–20 seconds.
- Second injection: Data repetition attack at 35–40 seconds.
- Third injection: Total data loss at 44–50 seconds.

Attack vectors are usually designed by the hackers to satisfy the observation model of (4). This would help them to by-pass attack detection in the control center. Additionally, attackers would tend to compromise as few measurements as possible in the effort to launch the attacks with the least effort. To successfully infiltrate the monitoring systems and the metering instrumentations, the attackers should have a detailed knowledge of the installed communication network protocols, substation automations, and physical design of digital relays [32–34]. The attack strategies are expected to be able to construct highly sparse attack vectors. Details about such stealthy sparse attacks were first discussed in [35]. In this paper, two methods are introduced to construct the sparse attack vectors under two typical scenarios: 1) random attacks in which arbitrary measurements can be compromised, and 2) targeted attacks in which the specific state variables need to be biased. Cyber-attacks can be generalized into 1) deception, and 2) denial of service. The deception refers to comprising the measurements from installed PMU in the grid. These examples include false data-injection and replay/repetition of past recorded measurements [36]. On the other hand, the denial of service is the action of jamming the communication channel causing the node to become unobservable. In the

TABLE III

TEST CASE II – OMAN ELECTRICITY GRID: DETECTING MULTIPLE OSCILLATIONS IN THE PRESENCE OF DATA-INJECTION ATTACKS

Time	**0 s–5 s**		**5 s–10 s**		**10 s–15 s**		**15 s–20 s**	
	ζ_{BAF}	f_{BAF}	ζ_{BAF}	f_{BAF}	ζ_{BAF}	f_{BAF}	ζ_{BAF}	f_{BAF}
	6.5	0.64	6.5	0.66	6.5	0.64	6.2	0.63
	5.4	0.75	5.4	0.74	5.4	0.75	5.6	0.76
	3.9	0.85	3.8	0.85	3.9	0.84	3.7	0.83
MSE	1.2×10^{-3}		1.2×10^{-3}		9.1×10^{-3}		1.8×10^{-3}	
Time	**20 s–25 s**		**25 s–30 s**		**30 s–35 s**		**35 s–40 s**	
	ζ_{BAF}	f_{BAF}	ζ_{BAF}	f_{BAF}	ζ_{BAF}	f_{BAF}	ζ_{BAF}	f_{BAF}
	6.5	0.63	6.5	0.62	6.5	0.62	6.3	0.66
	5.4	0.75	5.4	0.74	5.4	0.74	6.6	0.74
	3.9	0.85	3.9	0.84	0.9	0.86	4.1	0.84
MSE	3.0×10^{-3}		2.8×10^{-3}		2.5×10^{-3}		2.7×10^{-3}	
Time	**40 s–45 s**		**45 s–50 s**		**50 s–55 s**		**55 s–60 s**	
	ζ_{BAF}	f_{BAF}	ζ_{BAF}	f_{BAF}	ζ_{BAF}	f_{BAF}	ζ_{BAF}	f_{BAF}
	6.5	0.64	6.1	0.67	6.3	0.65	6.6	0.64
	5.4	0.75	5.5	0.72	5.3	0.74	5.5	0.74
	3.9	0.85	3.5	0.86	3.9	0.85	3.9	0.85
MSE	2.6×10^{-3}		8.7×10^{-3}		2.5×10^{-3}		2.4×10^{-3}	

literature, the cyber-attacks are addressed through evaluating a set of linear differential algebraic equations governed by the physical laws [36]. In the context of the oscillation monitoring application in WAMS, a signal-processing prospective of treating the electromechanical swings as a sum of exponentially damped sinusoidal waveforms was first proposed [37]. Such approach is not limited to a particular system model as required in the first option while allowing the system parameters to be extracted using the time-series analysis. The evaluation of detecting and identifying the cyber-attacks in WAMS has not been addressed before, and is crucial to the future of system operations.

This paper assumes a coordinated attack, where six PMUs are simultaneously subjected to the same data-injection attacks. Note the attacked PMUs are randomly selected, and are scattered across the entire Oman network. These six PMUs are Barka, Sur PS, Blue City, Al-Kamil, Filaj, and SPS substations. Among the attacked PMUs, Sur PS is a neighboring bus of the healthy PMU at Al-Kamil, Qurriyat is a neighboring bus of the healthy PMU at Wadi Adai, and Nizwa is a neighboring bus of the healthy PMU at Mannah. Since the distributed architecture considers the interaction between the neighboring nodes, the impact of the coordinated attacks on the neighboring healthy PMUs does not affect the overall monitoring results. This is also shown in our simulation results. The DFC will provide enhanced estimations of the oscillation parameters in the presence of data-injections. Note the number of healthy nodes should always be greater than the attacked nodes for the method to provide trust-worthy solutions. This assumption is true in most cases as it is difficult to hack the entire national grid at the same time.

Referring to Table III, high MSE errors are observed in the first 10 seconds. They are primarily due to the nature of the short-circuit fault. Here, the fault took place at a critical network location, which caused the transient effects to be felt throughout the entire system. Meanwhile, the second short-circuit event caused regional transient. Therefore, the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2016.2544854, IEEE Transactions on Smart Grid

distributed nature of the proposed scheme is able to extract more accurate results than the first fault. In terms of attack mitigation, it demonstrates strong resistance against data loss attacks. They are introduced to imitate denial-of-service attacks, which are effective ways to make operators lose network observability in certain regions. Although the system parameter and data-repetition attack better camouflage itself among actual measurements, the estimated oscillatory parameters from healthy PMUs allow these attacked PMUs to be identified and removed at the distributed fusion center. As a result, the MSE of the attacked windows is similar to the previous not attacked windows. Among all simulated attacks, the most threatening one is the injection of false damping ratio to the dominant inter-area oscillation which occurred in 15-20 second window. In this case, the lightly damped oscillation has been masked to exhibit adequate damping, thus damping ratio of 0.85 Hz has been replaced to 8%. This can lead to wide-area blackouts if the operators act on the false extracted monitoring results. Nevertheless, the proposed scheme shows decent rejection to this attack. The damping ratio of the 0.64 Hz oscillation was accurately estimated referring to Table III. A comparison of original profile of Barka substation and its recovery from attacks using the proposed scheme is illustrated in Fig. 5. The additional healthy monitoring nodes contribute to more accurate and prompt recovery of the attacked nodes. Overall, the proposed scheme demonstrates the ability to filter false system and recover parameters from any data-injection attacks while providing accurate monitoring results of the grid. The additional healthy monitoring nodes contribute to more accurate and prompt recovery of the attacked nodes. Overall, the proposed scheme demonstrates the ability to filter false system and recover parameters from any data-injection attacks while providing accurate monitoring results of the grid. Furthermore, the utilization of the distributed fusion center provides a global view for better Bayesian approximation of unobservable attacks at each local node. This minimizes the impacts of attacks on neighboring substations in the grid.

A time computation comparison has also been made with KF as shown in Table II. It can be seen that the proposed upper and lower bound schemes can reduce the computing time than KF. Compared to BAF, the upper and lower bound schemes were able to reduce the time computation by 13.84 % and 28.21 % respectively. Based on the overall observations and results, the upper and lower bound techniques have shown to improve the computation time in both test cases. However, there are no distinct advantages over each of the bounded techniques. Therefore, it is recommended that the proposed scheme should utilize both bounds of which can be implemented in a parallel computing architecture. The parallelization of both lower and upper bound can be made using multicore processors that are widely available in the mainstream market. However, this is not the scope of this work.

IV. Conclusions

In this paper, a Bayesian-based approximation filter has been proposed and demonstrated to improve the immunity of the monitoring applications against data-injection attacks. The predictive distribution property of the algorithm has helped to monitor power oscillation even in the presence of information loss. Mathematical derivations demonstrated the ability to identify attacks through interactions with neighboring monitoring nodes. In this paper, the proposed scheme has been applied to a mature wide-area monitoring application known as oscillation detection. Manipulating recorded and simulated measurements collected from Phasor Measurement Unit, the proposed method was able to extract accurate oscillatory parameters in the presence of data-injection attacks. Integration of the proposed immunity scheme in other WAMS applications will be evaluated in the future.

Appendix

A. Proof of Theorem II.1

Let us consider the lower bound at i-th node. Let $\underline{P}_t^i = \underline{P}_{t|t}^i$. $\psi_t = G_t^i Q_t^i G_t^{i^*}$, $\hat{\chi}_F^{ij} = \mathbf{E}[\chi_F^{ij}]$, and $\Phi = -(H_t^i \hat{\chi}_{F,t}^{ij} \underline{P}_t^i \hat{\chi}_{F,t}^{ij^*} H_t^{i^*} + H_t^i \psi H_t^{i^*} + R_{e,t}^i)^{-1}(H_{t^i} \psi_t + H_t^i \hat{\chi}_F^{ij} \underline{P}_t^i \hat{\Theta}^*)$.

Then based on Riccati difference equation [30], $\underline{P}_{t+1}$ can be expressed as:

$$\begin{aligned}\underline{P}_{t+1}^i &= \hat{\chi}_{F,t}^{ij} \underline{P}_t^i \hat{\chi}_{F,t}^{ij^*} + \psi_t - \Phi^*(H_t^i \hat{\chi}_{F,t}^{ij} \underline{P}_t^i \hat{\chi}_{F,t}^{ij^*} H_t^{i^*} + H_t^i \psi H_t^{i^*} \\ &\quad + R_{e,t}^i) \\ &= F_t^i(\hat{\chi}_{F,t}^{ij^*} + \hat{\chi}_{F,t}^{ij^*} H_t^* F_t^i)^* \underline{P}_t^i(\hat{\chi}_{F,t}^{ij^*} + \hat{\chi}_{F,t}^{ij^*} H_t^{i^*} \Phi) \\ &\quad + \Phi^*(H_t^i \psi H_t^{i^*} + R_{e,t}^i)\Phi_t + \psi H_t^{i^*} \Phi_t \\ &\quad + \Phi_t^* H_t^i \psi_t + \psi_t \end{aligned} \tag{38}$$

Hence, if $(\hat{\chi}_{F,t}^{ij^*} + \hat{\chi}_{F,t}^{ij^*} H_t^{i^*} \Phi)$ is not a stability matrix, for some $\underline{P}_0^i \leq P_{0|0}^i$. $\underline{P}_{t|t}^i$ diverges as $t \to \infty$. Since the state error covariance of the lower bound diverges and $\underline{P}_{t|t}^i \leq P_{t|t}^i$ for all $t \geq 0$, $P_{t|t}^i$ diverges as $t \to \infty$.

Acknowledgments

The authors thank Oman Electricity Transmission Company (OETC) for supplying the simulation models and Transpower New Zealand for providing the raw PMU data.

References

[1] A. Phadke and J. Thorp, "Synchronized phasor measurements and their applications," New York, NY, USA: Springer, 2008.
[2] C. Rehtanz, J. Bland, G. Benmouyal, S. Boroczky, C. Candia, D. Cirio, et al., "Wide area monitoring and control for transmission capability enhancement," *CIGRE Technical Brochure*, 2007.
[3] Xie, X., "WAMS applications in chinese power systems," *IEEE Pow. Ener. Mag.*, vol. 4, pp. 54-63, 2006.
[4] A. G. Tartakovsky, B. L. Rozovskii, R. B. Blaek, and H. Kim, "A novel approach to detection of intrusions in computer networks via adaptive sequential and batch-sequential change-point detection methods," *IEEE Trans. Sig. Proces.*, vol. 54, no. 9, pp. 3372–3382, Sep. 2006.
[5] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," *Proc. IEEE*, vol. 100, pp. 210–224, 2012.
[6] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "Interleaved hop-by-hop authentication against false data injection attacks in sensor networks," *IEEE Trans. Sen. Netwks.*, 2007.
[7] V. Shukla and D. Qiao, "Distinguishing data transience from false injection in sensor networks," *SECON*, 2007.
[8] Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks," *Proc. IEEE INFOCOM*, 2006.
[9] S. Cui et al., "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106–115, Sep. 2012.

[10] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[11] Y.-F. Huang, S. Werner, J. Huang, N. Kashyap, and V. Gupta, "State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid," *IEEE Sig. Process. Mag.*, vol. 29, no. 5, pp. 33–43, Aug. 2012.

[12] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, pp. 326–333, 2011.

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

[14] O. Kosut, L. Jia, R. J. Thomas, and L. Tong,"Limiting false data attacks on power system state estimation," *J. Fourier Anal. Appl.*, vol. 14, pp. 877–905, Dec. 2008.

[15] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," *Proc. 16th ACM Conf. Comput. Commun. Security*, 2009.

[16] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," *Proc. 49th IEEE Conf. Dec. Ctrl. (CDC)*, 2010, pp. 5991–5998.

[17] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," *Proc. 1st Workshop Secure Control Syst.*, 2010.

[18] O. Kosut, J. Liyan, R. J. Thomas, and T. Lang, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*,2010.

[19] F. Pasqualetti, F. Dorfler, F. Bullo, "Attack detection and identification in cyber-physical systems," *Automatic Control, IEEE Trans.*, vol. 58, no. 11, pp. 2715–2729.

[20] F. Pasqualetti, F. Dorfler, F. Bullo, "Control-theoretic methods for cyber-physical security: Geometric principles for optimal cross-layer resilient control systems," *Control Systems, IEEE Trans.*, vol. 35, no. 1, pp. 110–127.

[21] D. Karlsson, "Synchrophasor activities in CIGRE countries," *North American Synchrophasor Initiative Meeting*, 2010.

[22] A. Messina, "Inter-area oscillations in power systems," *NewYork: Springer*, 2009.

[23] G. Rogers, Power system oscillations, *Norwell*, MA: Kluwer, 2000.

[24] J. F. Hauer et al., "Initial results in Prony analysis of power system response signals," *IEEE Trans. Power Syst.*, vol. 5, no. 1, pp. 80–89, Feb. 1990.

[25] P. Pourbeik and C. Rehtanz, "Wide area monitoring and control for transmission capability enhancement," *Proc. CIGRE Working Group*, Jan. 2007.

[26] H. M. Khalid and J. C.-H. Peng, "Improved recursive electromechanical oscillations monitoring scheme: A novel distributed approach," *IEEE Trans. Pow. Syst.*, vol. 30, no. 2, pp. 680–688, Mar. 2015.

[27] N. Zhou, D. J. Trudnowski, J. W. Pierre, and W. A. Mittelstadt, "Electromechnical mode online estimation using regularized robust RLS methods," *IEEE Trans. Power Syst.*, vol. 23 no. 4, pp. 1670–1680, Nov. 2008.

[28] P. Korba, "Real-time monitoring of electromechanical oscillations in power systems: First findings," *IET Gen., Transm., Distrib.*, vol. 1, pp. 80–88, 2007.

[29] A. Ben-Israel and T. N. E. Greville, "Generalized Inverses: Theory and Applications," *2nd ed.*, 2002.

[30] Mosca, E., "Optimal, predictive, adaptive control," *New Jersey: Prentice-Hall*, 1995.

[31] O.E.T.C., "Five-Year Annual Transmission Capability Statement 2012-2016," Oman Electricty Transmission Company, 2012.

[32] M. Celikpala, and A. Han, "A primer on cyber security in Turkey and the case of nuclear power," *Technical Report, Center for Economics and Foreign Policy Studies, Turkey*, pp. 46–57, 2015.

[33] B. Kesler, "The vulnerability of nuclear facilities to cyber attack," *Strategic Insights*, vol. 10, no. 1, pp. 18, 2011.

[34] R. Brunt and D. Livingstone, "Cyber security at civil nuclear facilities understanding the risks," *Chatham House Report*, pp. 1–53, 2015.

[35] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *Proc. ACM Conf. Comput. Commun. Sec.*, pp. 21–32, 2009.

[36] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Auto. Ctrl.*, vol. 58, pp. 2715–2729, 2013.

[37] J. F. Hauer, "Application of Prony analysis to the determination of modal content and equivalent models for measured power system response," *IEEE Trans. Pow. Sys.*, vol. 6, pp. 1062–1068, 1991.

Haris M. Khalid (M'13) received the M.S. and Ph.D. degrees in control systems engineering from King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Kingdom of Saudi Arabia, in 2009 and 2012, respectively. He has worked as a Research Fellow with the Distributed Control Research Group, KFUPM.

Since 2013, he has been working as a Postdoctoral Researcher with the Department of Electrical Engineering and Computer Science, Institute Center for Energy, Masdar Institute of Science and Technology (MI), Masdar City, United Arab Emirates, collaborated with MI-MIT Cooperative Program. He has authored 40+ peer-reviewed publications, which includes 6 IEEE Transactions, 3 IET Journals, 2 Elsevier Journals, and 15+ peer-reviewed International Conferences. His research interests include power systems, cyber-physical systems, electric vehicles, signal processing, applied mathematics, fault diagnostics, filtering, estimation, performance monitoring, and battery management systems.

Jimmy C. -H. Peng (S'05-M'12) received the B.E. (Hons.) and Ph.D. degrees from the University of Auckland, Auckland, New Zealand, in 2008 and 2012, respectively. He then joined the Masdar Institute of Science and Technology (MI), Abu Dhabi, United Arab Emirates. In 2013, he was a Visiting Scientist with the Research Laboratory of Electronics at Massachusetts Institute of Technology (MIT), Cambridge, Massachusetts, and later a Visiting Assistant Professor with the MIT-MI Cooperative Program in 2014. Since 2016, he is an Assistant Professor with the Department of Electrical and Computer Engineering at the National University of Singapore, Singapore. His research interests include the control and identification techniques for electrical power grids, and their use in other cyber-physical systems.