Immunity Towards Data-Injection Attacks Using Multi-sensor Track Fusion-Based Model Prediction

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

***Abstract*—Utilization of synchrophasor measurements for wide area monitoring applications enables system operators to acquire real-time grid information. However, intentional injections of false synchrophasor measurements can potentially lead to inappropriate control actions, jeopardizing the security and reliability of power transmission networks. To resolve this issue, a multi-sensor track-level measurement fusion-based model prediction (TFMP) has been proposed. It has been demonstrated on a mature wide area monitoring application, which detect electromechanical oscillations. In this study, to extract the initial correlation information about attacked oscillation parameters, Kalman-like particle filter (KLPF)-based smoother has been used at each monitoring node. To reduce its computational burden, the KLPF-based smoother is diagonalized into subsystems. The scheme is further supported by the characteristics of moving horizon estimates (MHE) for handling continuous load fluctuations and perturbations caused by data-injections in power grids. Performance evaluations are conducted using different data-injection scenarios in the IEEE New England 39 Bus system. Results show the proposed TFMP accurately extracted oscillatory parameters from the contaminated measurements in the presence of multiple system disturbances and random data-injections.**

***Index Terms*—Kalman filter, inter-area oscillation, model prediction, multi-sensor data fusion, phasor measurement unit, power system stability, synchrophasor, track-level measurement fusion.**

I. INTRODUCTION

MODERN electrical grids demand accurate sensor measurements and communication channels to perform effective coordinated operations. Recent deployment of Phasor Measurement Units (PMUs) in transmission networks enables real-time grid dynamics to be recorded and transmitted to local data acquisition servers. Subsequently, signal processing algorithms can be applied to extract system information for online grid operations. However, the close coupling between cyber and physical operations can make system operations vulnerable to cyber-attacks [1, 2]. In this paper, the focus is towards cyber-attacks in the form of data-injections [1–10]. Abnormal data superimposed into collected synchrophasor measurements can cause false system information to be interpreted by installed monitoring algorithms. This can then lead to delays in mitigation actions. Among monitoring schemes using PMU measurements, state estimation and oscillation detection are more popular applications. Despite several methods are proposed for bad data detection in state estimation [4–6], none explored in the field of oscillation detection. Thus, the motivation of this paper improves the immunity of oscillation detection schemes against data-injections.

Power oscillations are electromechanical dynamics between synchronous generators in an interconnected grid. The frequency of local oscillation ranges from 0.8 to 2 Hz, while the frequency of intra-area mode are from 0.1 to 0.8 Hz [11, 12]. Inter-area oscillations are difficult to monitor and are prone in systems that are operating near their technical transfer capacity. As a result, monitoring algorithms to detect inter-area oscillation using synchrophasor measurements are proposed in recent time [12–18]. The objective is to detect lightly damped oscillations at early stage before they trigger angular and voltage instabilities. Inter-area oscillation was responsible for the North America northwestern blackout [12]. The present research trend is moving towards recursively monitoring oscillations under ambient situations. Recursive techniques can be categorized into 1) curve-fitting, and 2) an *a-priori* knowledge-based. The first refers to publications that extract oscillatory parameters directly from measurements [14–16]. The latter are associated with methods that approximate parameters using pre-

ACRONYMS AND ABBREVIATIONS OF MATHEMATICAL FORMULATIONS

KLPF	Kalman like particle filter
MHE	Moving horizon estimate
PMU	Phasor Measurement Unit
TEMP	Track-level fusion-based model prediction
TFC	Track fusion center
α	constant matrix with compatible dimensions
$f(.)$	nonlinear function for state transition model
x_0	initial condition of the oscillation state
w	random process noise
t	time instant
T	number of time instants
z	observation vector
p	number of synchrophasor observations
$h(.)$	nonlinear function for local observation matrix
x	state matrix for oscillations
υ	observation noise
N	number of sensors
X, **V**, **W**	Gaussian probability distribution function
ν	measurement noise
E	expectation operator
R_t	residual covariance
δ_{gh}	Kronecker delta
Q	process noise correlation factor
a_k,b_k	complex amplitudes of k-th mode
σ	damping factor
f	oscillatory frequency
T_s	sampling time
κ, $\mathit{\Psi}$, H^i	Jacobian matrices
$\tilde{x}$	linearized approximation of the system state
μ	mean
P	variance
$x_{1,t}$,$x_{2,t}$	states of subsystem 1 and 2
$\bar{\kappa}$, $\bar{\mathit{\Psi}}$, $\bar{H}$, $\bar{\upsilon}$	diagonalized variables
$P^{S_{1,2}}_{1,t\|t}$	smoothing error covariance of state $x_{1,t}$
$P^{S_{1,2}}_{2,t\|t}$	smoothing error covariance of state $x_{2,t}$
ϖ	interaction between subsystem 1 and 2
L, $\mathit{\Theta}$	positive functions
ξ	fault parameter
K_t	gain matrix
V	residual weighting matrix
$G(\omega)$	fault-free operating output
$G_f(\omega)$	faulty operating output
ω	frequency in rad/s
$c(\hat{G}(\omega), \hat{G}_f(\omega))$	magnitude-squared coherence spectrum
$test_{stat}$	test statistic

This work was funded by the Cooperative Agreement between the Masdar Institute of Science and Technology (MI), Abu Dhabi, UAE and the Massachusetts Institute of Technology (MIT), Cambridge, MA.

The authors are with Department of Electrical Engineering and Computer Science, Institute Center for Energy, MI, Abu Dhabi, UAE. E-mail: mkhalid, jpeng@masdar.ac.ae

vious knowledge of the system as well as the collected measurements [17]. An *a-priori* knowledge-based approach provides higher estimation accuracy under ambient or noisy conditions when accurate model is provided [18]. In this case, approximating electromechanical oscillations as a sum of exponentially damped sinusoidal signals is considered an accurate model representation in oscillation monitoring research [13]. Hence, the emphasis of this work is towards enhancing *a-priori* knowledge based techniques.

Despite published methods in oscillation detection can operate under noisy conditions, they are not proven to be resilient against data-injection attacks. Such attack is an emerging threat due to the increasing dependency of digital measurements for monitoring and control applications in recent years [7]. Majority of published monitoring methods are formulated based on the assumption of the measurements are not contaminated by human interventions. According to [3] and [8], cyber-attacks through introducing periodic or continuous bias to system measurements are possible. There are no guarantees that all cyber-attacks can be prevented. Any successful attack will cause existing monitoring schemes to generate inaccurate system information, which may then lead to cascading failures [7, 9, 10]. In recent literature, several methods are proposed to identify abnormal data segments and isolate attacked sensors [4, 7–10]. However, they usually require a large data batch and are computational intensive. Although an attacked sensor can be eventually identified, the time between the start of the attack until successful isolation can be in minutes or hours. This is a significant time window to trigger wide-area blackouts as operators are still being fed with false information. Referring to [12] and [19], it only takes minutes to make inter-area oscillation become lightly damped and generate wide area angular and voltage instabilities. Coming from the system operational perspective, the key objective is to minimize the potential damage of data-injection attack through novel processing of information collected from distributed sensors. To the authors' knowledge, such enhancement in oscillation monitoring algorithms has not been proposed.

Therefore, this paper contributes towards proposing a signal processing solution to enhance the resilience of existing oscillation monitoring methods against contaminated measurements. Since data-injection attacks in electrical grids can be considered as a regional event, the use of distributed architecture such as [18] is an adequate option against data contaminations. However, given the uncertainties of data-injection attack in the prescribed error statistics, it can be inappropriate to spend a huge amount of computational power to filter erroneous information as used by the algorithmic structure. Referring to [13], monitoring algorithms shall meet: 1) robustness against random fluctuations and bias, and 2) the computational cost of the propagation of estimation of each electromechanical oscillations. To achieve the robustness, while optimizing the computational complexity, constraints of perturbation and random fluctuations shall be considered. The aim is to maintain the accuracy of extracting oscillatory parameters as well as detecting potential monitoring nodes that are being attacked. In this paper, we integrated a modified KLPF-based smoother from [18] into the proposed track-level measurement fusion-based model prediction

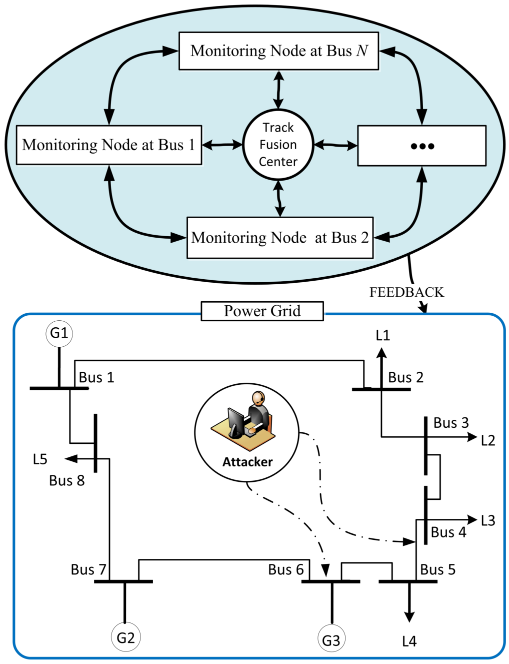

Fig. 1. Proposed TFMP scheme to estimate and detect data-injection attacks during power oscillations monitoring

(TFMP) approach. This concept is inspired from multi-sensor data fusion theory [21], and derived to support the formulation of providing immunity towards data-injection attacks. Here the track-fusion center represents the collection of measurements from all local sensors. The concept is developed in a distributed feedback environment.

To understand the integration of data-injection attacks into the oscillation monitoring application, an overview of the proposed multi-sensor TFMP is illustrated in Fig.1. The considered scenario assumed that the attacker is smart enough to inject data that can imitate regular variations of small-signal system dynamics. TFMP can resolve this concern by manipulating estimated oscillation parameters from all local sensor monitoring nodes. In this paper, a local sensor monitoring node refers to a site where KLPF-based smoother will be applied to extract oscillation parameters from PMU measurements collected at a substation. Furthermore, each monitoring node is assumed to be able to interact with its neighbors through substation communication channels. The estimated parameters are then communicated to the track fusion center and followed by track association and track fusion at the global level. Note the track fusion center is developed to compute and minimize the errors of filtering, prediction, and smoothing within each local sensor monitoring node.

The paper is organized as follows: The proposed scheme is formulated in Section II. In Section III the implementation and evaluation on a test case is discussed, and finally conclusions are drawn in Section IV.

Notations: In this paper, **E** is the expectation operator. A symbol $\hat{}$ over a variable indicates an estimate of that variable e.g. $\hat{x}$ is an estimate of x. 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, H_t, z_t). When any of these variables are collected from a subsystem 1 or 2, it will appear also as a part of subscript (e.g. $x_{1,t}$,

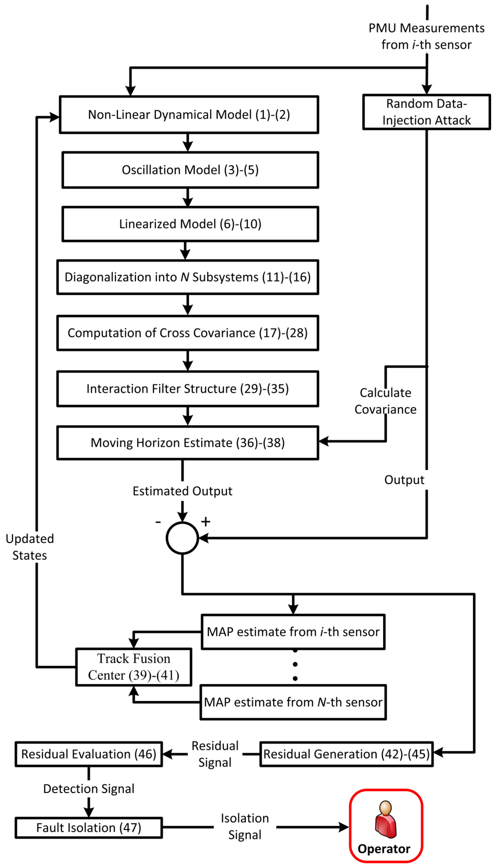

Fig. 2. Formulation framework of the proposed scheme

$x_{2,t}$, $H_{1,t}$, $H_{2,t}$, $z_{1,t}$, $z_{2,t}$). The notation x_0^T is used to denote the time sequence (e.g. x_0, x_1, ..., x_T).

II. The Proposed Scheme

This section derives the formulation of the proposed scheme. It begins with outlining the assumed system model, followed by the state representation of electromechanical oscillations. The TFMP algorithm is then built on it for calculating the estimates. An overview of the formulation framework of this section is illustrated in Fig. 2. It summarizes the formulation and equations involved at each step while tackling random data-injection attacks.

Note the formulation is derived from a perspective of a data-based approach. It is not restricted to linearized differential equations, which is merely a simplified model of the true system. In the field of real-time dynamic monitoring, especially for Wide Area Monitoring System (WAMS) applications, the notion is to become less dependent on classic models and adopt real-time system identification techniques. The reason is classic differential equations are less representative of continuous random load variations, line temperature variations, and other operational uncertainties. Although using differential equation based models are suitable for some steady-state or static applications like state estimation or automatic generation control, it is not suitable for monitoring electromechanical interactions of synchronous generators [13]. Therefore, system parameters are not extracted from offline predetermined power system models. Instead, the proposed method extract desired parameters from PMU measurements.

A. State Representation of Observation Model

A power grid prone to data-injection attacks can be expressed as a nonlinear dynamical system model. Perturbations and random fluctuations are part of noise-induced transitions in a nonlinear system with dynamics. It is expresses as:

$$\alpha x_{t+1} = f(x_t, w_t), \ t = 0, 1, ..., T \tag{1}$$

where α is the constant matrix with compatible dimensions to the model dynamics, $f(.)$ is the nonlinear function representing the state transition model, $x_0 \in \mathbf{R}^r$ is the initial condition of the oscillation state, superscript r is the size of the oscillation state vector in the subspace $\mathbf{R}$. In addition, $w_t \in \mathbf{R}^r$ is the random process noise, t is the time instant, and T is the number of time instants. Note Eq. (1) represents the equation of a system which has non-linear dynamics. Perturbations and random fluctuations are part of noise-induced transitions in a nonlinear system. These can be from load variations or switching transients of installed devices. Eq. (1) can also be represented by any other dynamical system model. It is not only limited to power systems.

It is assumed that the power grid described in (1) will be monitored by N number of synchronized sensors in a track-level measurement fusion environment. Computation is conducted at a central station, i.e. track fusion center (TFC), which involves control signals at each local node and predictive estimation sequences are generated in the presence of random noise fluctuations. These local sensors will basically be PMUs installed in high-voltage substations, and all will operate at the same sampling rate. The observations vector for extracting electromechanical oscillations at the i-th node possibly affected by the attack can be defined as:

$$z_t^i = h_t^i(x_t) + \upsilon_t^i, \ i = 1, ..., N \tag{2}$$

where $z_t^i \in \mathbf{R}^{p^i}$, p^i is the number of synchrophasor observations made by the i-sensor, $h^i(.)$ is a nonlinear function representing the local observation matrix of i-th sensor, x_t is the state matrix for oscillations, and $\upsilon_t^i \in \mathbf{R}^{p^i}$ is the observation noise of the i-th sensor. A dynamical power grid will be governed by the following constraints:

$$x_t \in \mathbf{X}_t, w_t \in \mathbf{W}_t, \upsilon_t \in \mathbf{V}_t \tag{3}$$

where $\mathbf{X}_t$, $\mathbf{V}_t$ and $\mathbf{W}_t$ are assumed to have Gaussian probability distribution function.

Assumption II.1: The noises w_t and ν_t are all initially assumed to be uncorrelated zero-mean white Gaussian such that $\mathbf{E}[w_t] = \mathbf{E}[\nu_t] = \mathbf{E}[w_g \nu_h^T] = 0, \forall t$. Note $\mathbf{E}$ denotes the expectation operator, and superscript $*$ denotes the transpose operator. Also, $\mathbf{E}[w_g w_h^T] = R_t \delta_{gh}$, $\mathbf{E}[\nu_g \nu_h^T] = Q_t \delta_{gh}$, $\forall t$, where R_t represents the residual covariance, δ_{gh} is a Kronecker delta which is one when variables g and h are the same. Q_t is the process noise correlation factor.

Once the observation model is constructed from synchrophasor measurements collected from the affected location, the corresponding state representation of electromechanical oscillations can then be formulated in the frequency domain.

B. Electromechanical Oscillation Model Formulation

Suppose a measured noise-induced signal contained K number of electromechanical oscillations. Referring to (2), the observation output signal z_t^i from an i-th sensor at time t can be modeled in the frequency domain as:

$$z_t^i = \sum_{k=1}^{K} a_k e^{(-\sigma_k + j2\pi f_k)tT_s} + \upsilon_t^i,\ t = 1, 2, ..., T \tag{4}$$

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 [17]. Eq. (2) has been transformed to Eq. (4), i.e. time domain to the frequency domain, using the Laplace transform. The system's poles and zeros are then analyzed in the complex plane. Moreover, it is especially important to transform the system into frequency domain to ensure whether the poles and zeros are in the left or right half planes, i.e. have real part greater than or less than zero. 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 for an i-th sensor as:

$$x_{k,t}^i = e^{(-\sigma_k + j2\pi f_k)tT_s},\ x_{k+1,t}^i = b_{k+1} e^{(-\sigma_{k+1} + j2\pi f_{k+1})tT_s} \tag{5}$$

The term b_k represents the complex amplitude of the k-th mode. Based on (5), a signal consisting of K number of exponentially damped sinusoids will be modeled by $2K$ number of states. Note that the k-th eigenvalue of a particular signal is described by two states denoted as $x_{k,t}$ and $x_{k+1,t}$, i.e. for k-th and $k+1$-th mode respectively. The eigenvalue represents the electromechanical oscillations between synchronous generators in the physical world. Details can be referred to [12, 13]. In addition, the damping factor σ_k and the corresponding frequency f_k of each oscillation will be computed from the state x_t. Estimating oscillatory parameters in the presence of a random data-injection attack will require the complete observability of the oscillation observation matrix. For a nominal case without data-injections, this was previously achieved by using an expectation maximization (EM) algorithm that utilized the initial correlation information extracted from KLPF [18]. Initial correlation information can be defined as the information collected from the initial estimates of the observation model $\hat{H}_t^0$. The superscript 0 represents the initial estimates. However, considering a data-injection attack situation, taking an averaged form of the log-likelihood function to improve estimate as in [18] is not sufficient. Instead, the initial correlation shall be iteratively calculated by 1) using the first and seconds moments of the input model for a node i, and then 2) getting *a-priori* information from the constraints, followed by 3) its observation estimates through time and frequency correlation for each i-th sensor. Note in this paper, monitoring power oscillation is used as an application. The proposed scheme can be utilized by any other application as well.

C. Initial Correlation Information

To estimate x_t in (1) and (2) from z_t^i at node i may be a difficult problem. This is both due to the nonlinear grid dynamics and the noise constraints outlined in (3). Referring to (1) and (2), a reasonable estimate will be to linearize the system to smooth-out nonlinearities. Thus the linearized model of the power grid will be:

$$f_t(x_t, w_t) \approx f_t(\tilde{x}_{t|t}, 0) + \kappa_t(x_t - \tilde{x}_{t|t}) + \Psi_t w_t \tag{6}$$

$$h_t^i(x_t) \approx h_t^i(\tilde{x}_{t|t-1}) + H_t^i(x_t - \tilde{x}_{t|t-1}) \tag{7}$$

where κ, Ψ, and H^i are the Jacobian matrices with compatible dimensions used to linearize the nonlinear dynamics:

$$\kappa_t = \frac{\partial}{\partial x} f_t(x, 0)|_{x=\hat{x}_{t|t}}, \Psi_t = \frac{\partial}{\partial w} f_t(\hat{x}_{t|t}, w)|_{w=0},$$
$$H_t = \frac{\partial}{\partial x} h_t(x, 0)|_{x=\hat{x}_{t|t-1}} \tag{8}$$

and $\tilde{x}_t$ is the linearized approximation of the system state x_t. This transformed (1) and (2) into:

$$\alpha x_{t+1} = \kappa x_t + \Psi w_t \tag{9}$$

$$z_t^i = H^i x_t + \upsilon_t^i,\ i = 1, 2, ..., N \tag{10}$$

where the oscillation system state $x_t \in \mathbf{R}^n$, the synchrophasor measurements $z_t^i \in \mathbf{R}^{m_i}$, $w_t \in \mathbf{R}^r$, and $\upsilon_t^i \in \mathbf{R}^{m_i}$. Variables α, κ, Ψ, and H^i are the constant matrices with compatible dimensions. The system model described by (9) and (10) is derived based on the following assumptions:

- $rank\, \alpha = n_1 < n$, and $rank\, \kappa \geq n_2$, where $n_1 + n_2 = n$.
- System (9) is regular, i.e. $det(s\alpha - \kappa) \not\equiv 0$, where s is an arbitrary complex number which can be expressed as a sum of real and imaginary components.
- The initial state x_0, with mean μ_0 and variance P_0, is independent of w_t^i and υ_t^i.

1) Diagonalization of the System Model at Node i into Subsystems:

Accurate monitoring of power oscillations in the presence of data-injection attacks can prove to be computational expensive. However, to tackle the additional computational cost due to the calculation of initial estimates and the error covariance matrix $P_{t|t-1}$ may be demanding. This is due to the size of error covariance matrix which is equal to the size of the state vector, and therefore directly proportional to the size of the modelled power grid. To reduce the computational cost of the initial estimates and the error covariance matrix, diagonalizing the main system model into subsystems is proposed. This is derived on the structure for the KLPF-based smoother which can be referred to (19)-(26) in [18]. In [18], the KLPF-based smoother $\hat{x}_{t|t}^S$ of the state x_t is calculated based on measurements $(z_t^i, ..., z_T^i)$. Note the attacked system at node i can be diagonalized up to N number of subsystems. To simplify the formulation, diagonalization of $N = 2$ subsystems is considered in this paper. This reflects that each i-th node consists of two subsystems. Using the theory of robust eigenvalue assignment from [22], the system described by (9) and (10) can be decomposed into L and R non-singular matrices.

$$L\alpha R = \begin{bmatrix} \alpha_1 & 0 \\ \alpha_2 & 0 \end{bmatrix}, L\kappa R = \begin{bmatrix} \kappa_1 & 0 \\ \kappa_2 & \kappa_3 \end{bmatrix}, L\Psi R = \begin{bmatrix} \Psi_1 \\ \Psi_2 \end{bmatrix}, H^i R = \begin{bmatrix} H_1^i \\ H_2^i \end{bmatrix}^* \tag{11}$$

where $\alpha_1 \in \mathbf{R}^{n_1 \times n_2}$ is non-singular lower-triangular, $\kappa_1 \in \mathbf{R}^{n_1 \times n_1}$ is quasi-lower-triangular, $\kappa_3 \in \mathbf{R}^{n_2 \times n_2}$ is non-singular lower-triangular. Transforming $x_t = R\,[x_{1,t}^*\ x_{2,t}^*]^*$, where $x_{1,t} \in \mathbf{R}^{n_1}$, $x_{2,t} \in \mathbf{R}^{n_2}$. The system can be transformed into the following two diagonalizable subsystems by taking the inverse of high dimensional matrices of (1) and (2) using a linear minimum variance [23]:

$$x_{1,t+1} = \kappa_0 x_{1,t} + \Psi_0 w_t \tag{12}$$

$$x_{2,t} = \bar{\kappa} x_{1,t} + \bar{\Psi} w_t \tag{13}$$

$$z_t^i = \bar{H}_t^i x_{1,t} + \bar{v}_t^i \tag{14}$$

where $x_{1,t}$ and $x_{2,t}$ are the states of subsystem 1 and subsystem 2, respectively. κ_0, Ψ_0, $\bar{\kappa}$, $\bar{\Psi}$, $\bar{H}$ and $\bar{v}$ are diagonalized variables, which are computed from the inverse of weighted matrices α_1 and κ_3 as shown in the Appendix. In the subsystem transformation, only first subsystem will have the prediction and filtering stage, whereas the rest of $N-1$ subsystems will only have filtering stage. Referring to (12)–(14), the resultant noises $\bar{w}_t$ and $\bar{v}_t$ will have the diagonalizable expected value:

$$\mathbf{E}\{\begin{bmatrix} \bar{w}_t \\ \bar{v}_t^1 \end{bmatrix}, \begin{bmatrix} \bar{w}_t^* \; \bar{v}_t^{2^*} \end{bmatrix}\} = Q_t^{1,2} \delta_t^{1,2} \tag{15}$$

where $Q_t^{1,2}$ is the process noise correlation factor between subsystem 1 and 2, $\delta_t^{1,2}$ is the Kronecker delta function used for shifting the integer variable after the presence or absence of noise. $Q_t^{1,2}$ can be expressed as:

$$Q_t^{1,2} = \begin{bmatrix} Q_{\bar{w}} & \alpha^2 \\ \alpha^{1^*} & Q_{\bar{v}^{1,2}} \end{bmatrix} \tag{16}$$

where $\alpha^1 = Q_{\bar{w}}\, \Psi_3^{i^*}$, $Q_{\bar{v}^i} = \Psi_3^i \, Q_{\bar{w}} \, \Psi_3^{i^*} + Q_{v^i}$ and $Q_{\bar{v}^{1,2}} = \Psi_3^i \, Q_{\bar{w}} \, \Gamma_3^{i^*}$, Ψ_3^i is defined in the Appendix.

Once the subsystems are constructed from the system affected by the data-injection attacks, the interactions between them shall be evaluated. This will require extracting the signature of random variations, which can be obtained by comparing measurements with known system dynamics. This interaction is evaluated here by using cross-covariance analysis. It is proposed to improve the goodness of fit of random variations, while enhancing the predictive accuracy and covariance estimates of the KLPF.

D. Computation of Cross-covariance

From (12)-(16) and considering (19)-(26) in [18], the state of subsystem 1, $x_{1,t}$, and subsystem 2, $x_{2,t}$ can be derived. This is to have complete observability on the dynamics of power oscillations in the presence of random data-injection attacks. First, suppose the *a-priori* equation of state $x_{1,t}$ at node i is computed as:

$$\tilde{x}_{1,t+1|t}^i = \bar{\kappa}_0^i (I_{n_1} - \beta_t^i \bar{H}_t^i) \tilde{x}_{1,t|t-1}^i + \Psi_0 w_t - (\bar{\kappa}_0^i \beta_t^i + J^i) \bar{v}_t^i \tag{17}$$

where $\tilde{x}_{1,t|t-1}^i$ is the difference between $x_{1,t}$ and $\hat{x}_{1,t|t-1}^i$, $\bar{\kappa}_0^i = \kappa_0 - J^i \bar{H}_t^i$, $J^i = \Psi_0 \alpha^i Q_{\bar{v}^i}^{-1}$, $\kappa_t^i = \bar{\kappa}(I_{n_1} - \beta_t^i \bar{H}_t^i) - \bar{\Psi} \alpha^i Q_{\varepsilon^i,t}^{-1} \bar{H}^i$. I_{n_1} is an $n_1 \times n_1$ identity matrix. For notation convenience, $\beta_t^i = \frac{P_t^i H_t^{i^*}}{H_t^i P_t^i H_t^{i^*} + \sigma_v^2}$. The corresponding updated *a-posteriori* equation of state $x_{1,t}$ at node i will be:

$$\tilde{x}_{1,t|t}^i = (I_{n_1} - \beta_t^i \bar{H}_t^i) \tilde{x}_{1,t|t-1}^i - \beta_t^i) \bar{v}_t^i \tag{18}$$

where $\tilde{x}_{1,t|t}^i$ is the difference between $x_{1,t}$ and $\hat{x}_{1,t|t}^i$. Thus, the updated and predicted error equations of state $x_{1,t}$ are achieved. The state $x_{2,t}$ of second diagonalized subsystem at node i can also be expressed as:

$$\tilde{x}_{2,t|t}^i = F_t^i \tilde{x}_{1,t|t-1}^i + D_t^i [\bar{w}_t^*, \bar{v}_t^{i^*}]^* \tag{19}$$

where $\tilde{x}_{2,t|t}^i = x_{2,t} - \hat{x}_{2,t|t}^i$, $F_t^i = \bar{\kappa}(I_{n_1} - \beta_t^i \bar{H}_t^i) - \bar{\Psi} \alpha^i Q_{\varepsilon^i,t}^{-1} \bar{H}_t^i$ and $D^i = [\bar{\Psi} - \bar{H}_t \beta_t^i - \bar{\Psi} \alpha^i Q_{\varepsilon^i,t}^{-1}]$. Once the subsystem states are derived, the cross-covariance between them can be formulated to filter any random variations caused due to the attack within collected synchrophasor measurements.

1) Cross-covariance of State $x_{1,t}$ (12) for Subsystem 1:

Using the projection theory proposed in [24], cross-covariance equation of the prediction and filtering errors of state $x_{1,t}$ between the subsystems 1 and 2 of the i-th node can be computed as:

$$P_{1,t+1|t}^{1,2} = \bar{\kappa}_0^1 [I_{n_1} - \beta_t^1 \bar{H}_t^1] P_{1,t|t-1}^{1,2} [I_{n_1} - \beta_t^2 \bar{H}_t^2]^* + [\Psi_0 - \bar{\kappa}_0^1 \beta_t^1 - J^1] Q^{1,2} [\Psi_0 - \bar{\kappa}_0^2 \beta_t^2 - J^2]^* \tag{20}$$

where the subscript 1 and 2 represents the subsystem 1 and 2 for i-th node, respectively. The initial value of $P_{1,t+1|t}^{1,2}$ is $P_{1,0|t}^{1,2}$. which is the first $n_1 \times n_1$ block of $R^{-1} P_{1,0|0}^{1,2} R^{-1^*}$. Subsequently, the error equation of the updated *a-posteriori* estimates will be:

$$P_{1,t|t}^{1,2} = [I_{n_1} - \beta_t^1 \bar{H}_t^1] P_{1,t|t-1}^{1,2} [I_{n_1} - \beta_t^2 \bar{H}^2]^* + \beta_t^1 Q_{\bar{v}^{1,2}} \beta_t^2 \tag{21}$$

2) Cross-covariance of State $x_{2,t}$ (13) for Subsystem 2:

The covariance matrix of the filtering errors for state $x_{2,t}$ between the subsystem 1 and 2 for the i-th node can be expressed as:

$$P_{2,t|t}^{1,2} = F_t^1 P_{1,t|t-1}^{1,2} F_t^{2^*} + D_t^1 Q^{1,2} D_t^{2^*} \tag{22}$$

where $P_2^{1,2}(t|t)$ is the filtering error covariance of $x_{2,t}$ based on the subsystem 1 of i-th node .i.e. $P_{2,t|t}^1$.

Considering the cross-covariance computation of subsystem 1 and 2, the smoother of [18] is re-derived here to further improve the estimation of suboptimal correlation information provided by the diagonalized subsystems. Moreover, the estimated output of the smoother will be more superior in providing insight to the power oscillation dynamics to those obtained from the subsystem 1 and 2 as it extrapolates backwards in time.

3) Cross-covariance of Smoothing:

The cross-covariance of the smoothed *a-posteriori* estimate between the subsystem 1 and 2 of the i-th nodes are extended on (25)-(26) from [18]. The state estimate $\hat{x}_{t|T}$, given the whole time sequence, can be represented as:

$$\hat{x}_{t|T}^{1,2} = \hat{x}_{t|t-1}^{1,2} + P_{t|t-1}^{1,2} r_{t|T}^{1,2} \tag{23}$$

where $t = N-1, N-2, ..., 1$. Here r is an $n \times n$ vector that satisfies the backward recursive equation where $r_{T+1|T} = 0$. $P_{t|T}^{\alpha_{1,2}}$ is the covariance matrix of $r_{t|T}$ with a size of $n \times n$ and satisfies the backward recursive equation. The resultant cross-covariance of $r_{t|T}$ will be:

$$r_{t|T}^{1,2} = \bar{\kappa}_p^{1^*} [I_{n_1} - \beta_t^{1,2} \bar{H}_t^2] r_{t|t-1} + H^{2^*} [H^2 P_{t|t-1}^{1,2} H_t^{2^*} + R_t]^{-1} (\tilde{z}_{t+1}^2 - \tilde{H}_{t+1}^2 \tilde{x}_{t+1}^2) \tag{24}$$

where $\kappa_{t+1|t} = \kappa_{t+1|t}[I - K_t H_t]$. According to the smoothing property, the covariance matrix $P_{t|T}$ shall depend on of the time sequence T such that:

$$P_{t|T}^{1,2} = P_{t|t-1}^{1,2} - P_{t|t-1}^{1,2} P_{t|T}^{S_{1,2}} P_{t|t-1}^{1,2} \tag{25}$$

This is followed by the smoothed-run updated *a-posteriori* estimate, which will update the error covariance matrix in the smoothed run:

$$P^{S_{1,2}}_{t|T} = \bar{\kappa}^{1^*}_p [I_{n_1} - \beta^{1,2}_t \bar{H}^2]^* P^{\alpha_{1,2}}_{t|t-1} \bar{\kappa}^2_p [I_{n_1} - \beta^{1,2}_t \bar{H}^1] + H^{1^*}[H^2 P_{t|t-1} H^{2^*} + R_t]^{-1} H^2 \quad (26)$$

The derived cross-covariance matrices for smoothing the state x_t between subsystem 1 and 2 are:

$$P^{S_{1,2}}_{1,t} = I_{n_1} P^{1,2}_{1,t} I^*_{n_1} + (H^1 P_{t|t-1} H^{2^*})^{-1} \quad (27)$$

$$P^{S_{1,2}}_{2,t} = F^1_t P^{1,2}_{1,t} F^{2^*}_t + D^1_t (H^1 P_{t|t-1} H^{2^*})^{-1} D^{1^*}_t \quad (28)$$

where $P^{S_{1,2}}_{1,t|t}$ and $P^{S_{1,2}}_{2,t|t}$ are the smoothing error covariance of state $x_{1,t}$ and $x_{2,t}$ respectively. Up to now, the formulations of the cross-covariance for prediction, filtering and smoothing error for the subsystems are derived. The next step will be to combine them into an interaction filter so that the variance of interaction errors among the state $\hat{x}^{\varpi}_{2,t|t}$ can be determined.

4) Interaction filter Structure based on Cross-covariance Computation:

Based on (12)-(14) for subsystem 1 and 2, the interacted filter can be stated for state $x_{1,t}$ of subsystem 1 as:

$$\hat{x}^{\varpi}_{1,t|t} = (e^*_{1,t} \Upsilon^{-1}_{1,t} e_{1,t})^{-1} e^*_{1,t} \Upsilon^{-1}_{1,t} [\hat{x}^{i^*}_{1,t}, \hat{x}^{i^*}_{2,t}, ..., \hat{x}^{N^*}_{1,t|t}] \quad (29)$$

where superscript ϖ denotes the interaction between subsystem 1 and 2. $e_{1,t} = [I_{n,1}, ..., I_{n,1}]$ is an $n_1 N \times n_1$ matrix, $\Upsilon_{1,t} = P^{1,2}_{1,t|t}$ is an $n_1 N \times n_1 N$ positive definite matrix. Similarly, the resultant diagonalized interacted filter for state $x_{2,t}$ of subsystem 2 became:

$$\hat{x}^{\varpi}_{2,t|t} = (e^*_{2,t} \Upsilon^{-1}_{2,t} e_{2,t})^{-1} e^*_{2,t} \Upsilon^{-1}_{2,t} [\hat{x}^{i^*}_{1,t}, \hat{x}^{i^*}_{2,t}, ..., \hat{x}^{N^*}_{2,t|t}] \quad (30)$$

where $e_{2,t} = [I_{n,2}, ..., I_{n,2}]$ is an $n_2 N \times n_2$ matrix. $\Upsilon_{2,t} = P^{1,2}_{2,t|t}$, is an $n_2 N \times n_2 N$ positive definite matrix. Variances of $\hat{x}^{\varpi}_{1,t|t}$ and $\hat{x}^{\varpi}_{2,t|t}$ are given by:

$$P^{\varpi}_{1,t|t} = (e^*_1 \Upsilon^{-1}_{1,t} e_1)^{-1}, \; P^{\varpi}_{2,t|t} = (e^*_2 \Upsilon^{-1}_{2,t} e_2)^{-1} \quad (31)$$

where $P^{\varpi}_{1,t|t} \leq P^i_{1,t|t}$ and $P^{\varpi}_{2,t|t} \leq P^i_{2,t|t}$. Restoring the variances of (12)-(14) to the main singular system described by (9) and (10) made the filter into:

$$\hat{x}^{\varpi}_{t|t} = R[\hat{x}^{\varpi^*}_{1,t|t} \, \hat{x}^{\varpi^*}_{2,t|t}]^* \quad (32)$$

The variance of the filtering error of $\hat{x}^{\varpi}_{t|t}$ in (32) can be computed by:

$$P^{\varpi}_{t|t} = R \begin{bmatrix} P^{1,2}_{1,t|t} & P^{1,2}_{12,t|t} \\ P^{1,2}_{21,t|t} & P^{1,2}_{2,t|t} \end{bmatrix} R^* \quad (33)$$

where covariance matrix $P^{1,2}_{1,t|t}$ and $P^{1,2}_{2,t|t}$ are computed by (21) and (22), respectively. The covariance matrix $P^{\varpi_{1,2}}_{t|t}$ between filtering errors $\tilde{x}^{\varpi}_{1,t|t}$ and $\tilde{x}^{\varpi}_{2,t|t}$ can then be defined as:

$$P^{\varpi_{1,2}}_{t|t} = P^{\varpi}_{1,t|t} e^*_1 \Upsilon^{-1}_{1,t} \Upsilon^{1,2}_t \Upsilon^{-1}_{2,t} e_2 P^{\varpi}_{2,t|t} \quad (34)$$

where $P^{\varpi_{1,2}}_{t|t} = P^{\varpi^*_{2,1}}_{t|t} =$ and $\Upsilon^{1,2}_t = P^{1,2}_{t|t}$. $P^{1,2}_{t|t}$ can be computed as follows:

$$P^{\varpi_{1,2}}_{t|t} = (I_{n_1} - \beta^1_t \bar{H}^1_t) P^{1,2}_{1,t|t-1} F^{2^*}_t + [0, -\beta^1_t] Q^{1,2} D^{2^*} \quad (35)$$

where $P^{1,2}_{t|t} = P^{2,1^*}_{t|t}$. Likewise, the variance of smoothing error of $\hat{x}^S_{t|t}$ is computed by (26).

The developed diagonalized interacted filters will be used to determine the initial correlation information. However, up to now, the initial correlation information has not considered the constraints outlined in (3). This means the initial correlation will only be good enough to give the first estimates of the oscillation monitoring procedure, where its performance is enhanced by computing the interaction parameter between the subsystems. To take the constraints into account, the maximum *a-posteriori* (MAP) estimate shall be calculated. Note that by handling the noise and state constraints of (3), the immunity of the estimation results during data-injection can be increased. To achieve this, a moving horizon estimate (MHE) is proposed. It involved a state prediction stage to mitigate data-injection attacks.

E. Moving Horizon Estimate (MHE)

Given the observation measurement sequence $(z_1, ...z_T)$ at time t, the MAP criteria for calculating the oscillation estimate with constraints can be expressed as:

$$\hat{x}^{\text{MAP}}_t = \arg \max_{x_0......x_T} p(x_0......x_T | z_0, ...z_{T-1}) \quad (36)$$

Considering the constraints (3) and the observation vector (2), the log-likelihood is implemented with state variables as:

$$= \arg \min_{x_0,....,x_T} \sum_{t=0}^{T-1} ||\upsilon||^2_{R^{-1}_t} + ||w_t||^2_{Q^{-1}_k} + ||x_0 + \bar{x}_0||^2_{P^{-1}_0} \quad (37)$$

Considering (37), the minimization problem can be formulated as:

$$\min_{x_0, w_t, \upsilon_t} \sum_{t=0}^{T-1} L_t(w_t, \upsilon_t) + \Theta(x_0) \quad (38)$$

where L_t and Θ are positive functions, and $L_t(w_t, \upsilon_t) = ||\upsilon||^2_{R^{-1}_k} + ||w_t||^2_{Q^{-1}_t}$, $\Theta(x_0) = ||x_0 - \bar{x}_0||^2_{P^{-1}_0}$. The MAP estimate from each local i-th sensor can then be gathered. Using previously derived expressions and computed information, the track fusion architecture can now be established.

F. Track Fusion Center (TFC)

The TFC functions to estimate oscillatory parameters from all the local monitoring nodes in the presence of data-injection attacks. Its purpose is to improve the accuracy of the covariance and estimated states in each node. Subsequently, all local sensor observations from N number of sensors are integrated into the track observation vector $z^{\text{TF}}_t \in \mathbf{R}^{p_{\text{TF}}}$. The superscript TF denotes the track fusion, and p_{TF} is the track fusion-based observation measurements collected from N number of sensors. Thus, the track fusion-based observation model at time-instant t can be represented as,

$$z^{\text{TF}}_t = H^{\text{TF}}_t x_t + w^{\text{TF}}_t, \quad (39)$$

Similar to (2), the corresponding observation model is H^{TF}_t, and the noise vector is w^{TF}_t. They can also be expressed as an array of information collected from all substations as $z^{\text{TF}}_t = [z^1_t, ...z^N_t]^*$, $H^{\text{TF}}_t = [H^1_t, ...H^N_t]^*$, $w^{\text{TF}}_t = [w^1_t, ...w^N_t]^*$, where N is the number of sensors. Considering the track estimation-based variables z^{TF}_t, H^{TF}_t, and w^{TF}_t, the oscillation state estimate at TFC can be presented as:

$$\hat{x}^{\text{TF}}_{t|t} = P^{\text{TF}}_{t|t} \sum_{i=1}^{N} P^{i^{-1}}_{t|t} \hat{x}^i_{t|t} \quad (40)$$

where $P_{t|t}^{\text{TF}} = [\sum_{i=1}^{N} P_{t|t}^{i^{-1}}]^{-1}$. Apart from calculating the cross-covariance computation of subsystems at each i-th node, TFC also calculated the interactions of neighboring sensors. Considering the interactions between local sensors, the covariance matrix for i-th and j-th sensors can be expressed as:

$$P_{t|t}^{ij} = \mathbf{E}[\tilde{x}_{t|t}^{i} \tilde{x}_{t|t}^{j^*}] = [1 - w_t^i H_t^i] P_{t|t-1}^{ij} [1 - w_t^j H_t^j]^* \quad (41)$$

where $\tilde{x}_{t|t} = x_{t|t} - \hat{x}_{t|t}$. This is derived based on the same principles as the covariance of the subsystems within one monitoring node. Hence, $P_{t|t-1}^{ij}$ can be calculated based on the diagonalized subsystem variance by (33), while its smoothed variance by (26). The TFC will provide estimation of the oscillation parameters in the presence of data-injections. To detect the occurrence of injected data, residuals can be continuously generated and evaluated from each sensor.

Note the track fusion center receives tracked measurements from each sensor node. This may cause processing and communication delays between local sensors and fusion center. This delay has been tackled by the model-prediction property of the proposed scheme. It can be observed from Eq. (36)-(38) that the moving horizon estimate (MHE) considers the whole time sequence for the calculation of model-prediction. This idea covers any time-delays which are actually measurement delay less than, equal to, or more than one sampling period. Moreover, to tackle this problem at a large-scale, the delayed measurements can be determined by deriving the cross-covariance for each delayed measurement and at each time interval.

G. Generation and Evaluation of Residuals for detecting Data-Injection Attacks:

The residual of the estimated parameters is generated to detect any variations due to system-bias and injected faults. To detect variations from a residual generation for each measurement, there exists L_0 such that for any norm bounded $x_{1,t}, x_{2,t} \in \mathbf{R}^n$, the inequality $\|(u_t, z_t, x_{1,t}) - (u_t, z_t, x_{2,t})\| \leq L_0 \|x_{1,t} - x_{2,t}\|$ holds. Considering the simplified form of system as (9), the transfer function matrix $H_t[sI - (\kappa_t - K_t H_t)]^{-1} \Psi_t$ is strictly positive real, where $K_t \in \mathbf{R}^{n \times r}$ is chosen such that $A_t - K_t H_t$ is stable. Thus, the following expression is constructed as:

$$\hat{x}_t = \kappa \hat{x}_t + (u_t, z_t) + \xi_{f,t}(u_t, z_t, \hat{x}_t) + K_t(z_t - \hat{z}_t) \quad (42)$$

where $\xi_t \in \mathbf{R}$ is a parameter that changes unexpectedly when a fault occurred, K_t is the gain matrix. $\hat{z}_t = H_t \hat{x}_t$ and $r_t = V(z_t - \hat{z}_t)$, where the variable V is the residual weighting matrix. Since the pair (κ_t, H_t) is assumed to be observable, K_t can be selected to ensure $\kappa_t - K_t H_t$ will be a stable matrix. This can be defined as:

$$e_{x,t} = x_t - \hat{x}_t, \quad e_{z,t} = z_t - \hat{z}_t \quad (43)$$

Error equations will then become:

$$e_{x,t+1} = (\kappa_t - K_t H_t) e_{x,t} + [\xi_t(u_t, z_t, x_t) - \xi_{f,t}(u_t, z_t, \hat{x}_t)] \quad (44)$$

$$e_{z,t} = H_t e_{x,t} \quad (45)$$

Once the residual is found, evaluations are required to determine the threshold selection for identifying a fault.

The residual evaluation is performed by a coherence function [25, 26]. A function based on magnitude of squared coherence spectrum is employed to determine the fault-injection status of a power grid at its outputs. Let $\hat{G}(\omega)$ and $\hat{G}_f(\omega)$ be the estimates of the frequency response of the power grid under normal fault-free and faulty operating output regimes, respectively. Here ω is the frequency in rad/s. The magnitude-squared coherence spectrum of the two signals can be defined as:

$$c(\hat{G}(\omega), \hat{G}_f(\omega)) = \frac{|\hat{G}(\omega)\hat{G}_f(\omega)|^2}{|\hat{G}(\omega)|^2 |\hat{G}_f(\omega)|^2} \quad (46)$$

where $c(\hat{G}(\omega), \hat{G}_f(\omega))$ is the magnitude-squared coherence spectrum, and $\hat{G}^*(\omega)$ is the complex conjugate of $\hat{G}(\omega)$. In the presence of noise, a threshold value is estimated to give a high probability of detection and a low probability of false alarms. The test statistic $test_{stat}$ is chosen to be the mean value of the coherence spectrum $test_{stat} = \mu_{1/2}(c(\hat{G}(\omega), \hat{G}_f(\omega)))$ as:

$$test_{stat} = \begin{cases} \leq th \, \forall \omega \in \Omega \; fault \\ > th \, \forall \omega \in \Omega \; no\, fault \end{cases} \quad (47)$$

where $0 \leq th \leq 1$ is a threshold value, Ω is the relevant spectral region, e.g. bandwidth. This gives the coherence function-based thresholds for detection of fault-injections.

III. Implementation and Evaluation

Validation of the proposed TFMP estimation scheme is conducted using simulated synchrophasor measurements collected from IEEE 39-Bus New England system shown in Fig. 3. Modeling details are based on [27, 28]. In this study, synchrophasor measurements are collected from Bus 15, 16, 17, 29, 30, 35, 37, 38, and 39. From these data, three dominant electromechanical modes are detected using Welch power spectral density. Their pre-disturbance values are: 1) 0.69 Hz with a damping ratio of 3.90%, 2) 1.12 Hz with a damping ratio of 5.71%, and 3) 1.17 Hz with a damping ratio of 5.62%. The 0.69 Hz mode will be considered as an inter-area oscillation. All loads are continuously being subjected to random small magnitude fluctuations of up to 10 MW per second. Furthermore, the system is excited by four large-signal disturbances over a period of 60 seconds. Firstly, a three-phase-to-ground fault occurred at Bus 24 at 5 second and is cleared after 0.1 second. Secondly, the active and reactive power demands of the load connected at Bus 21 is ramped up by 30% and 10% over ten seconds, respectively. Thirdly, the line connecting Bus 16 and 17 is disconnected at 25 second and reconnected after 5 seconds. Lastly, the active and reactive load demands at Bus 4 increased by 20% and 10%, respectively. This occurred over a 5 second ramp. All simulations are performed using DIgSILENT PowerFactory Ver. 15.1 [29]. From the collected measurements, monitoring schemes updated the averaged oscillatory parameters every 5 second. In this study, the proposed method is evaluated against the distributed technique of [18].

To simulate deliberate attack scenarios, data-injections are carried out in the collected synchrophasor measurements. Since all three electromechanical modes are observable at Bus 16 and 17, these two locals are selected as attack nodes. Their neighboring nature shown in Fig. 3 helped to create a situation of regional attacks on measured data. Simulated attack scenarios at Bus 16 and Bus 17 are:

- First injection: Random data-injections are introduced at Bus 16 from 7 to 12 seconds.

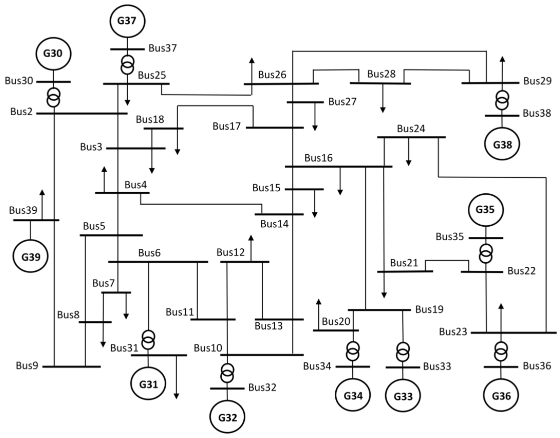

Fig. 3. Single line diagram of the IEEE 39-Bus New England System

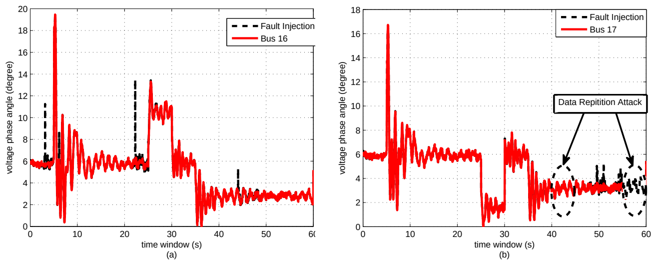

Fig. 4. Profile of a) Bus 16 and b) Bus 17 with random fault injections

- Second injection: Signal with relatively high energy potency are injected at Bus 16 from 22 to 27 seconds.
- Third injection: Small signature of random sinusoidal waveforms are introduced at Bus 16 during 44 to 49 seconds. Also, ambient disturbance-like injections are introduced at Bus 17 during 48 to 55 seconds.
- Fourth injection: Small signature of random sinusoidal waveforms are introduced at Bus 16 during 44 to 49 seconds. Also, a data-repetition attack was introduced at Bus 17 from 55 to 60 seconds. This attack replaces the normal oscillation behavior with those recorded at Bus 17 from 40 to 45 seconds.

The first injection illustrates a pure random attack with no bias towards any signal characteristics. The second injection imitates an attack attempting to bring down a local/regional network. The third injection represents an ambient attack with the aim to generate a cascading failure in the longer form that can often led to wide-area blackouts. Ambient disturbance-like injections are also introduced at Bus 17 to create a multi-sensor injection attack situation as part of the third injection scenario. The fourth injection represents a data-repetition attack at Bus 17. The purpose of injecting different nature of signals and at multiple locations are to assess the robustness of the proposed scheme. These data segments, outlined in black, are added to the original synchrophasor measurements, colored in red, as shown in Fig. 4a and 4b.

The monitoring performance is summarized in TABLE I. Firstly, the tracking performance in windows without the presence of data-injections are discussed. Overall, both methods are able to accurately estimate all three electromechanical parameters. A slight increase in mean squared error (MSE) values for the distributed method is observed between 30 to 40 second period. They are in par with the case of the line outage event in the previous time window. The reason can be due to the dominance of non-linear dynamics in the measurements, which caused the linear-based distributed monitoring scheme to struggle. In contrast, the proposed scheme is less influenced due to its cross-covariance computation at each local sensor. Overall, both methods generated low MSE while the proposed TFMP estimation scheme achieved higher accuracy. Next, the performance under deliberate data-injections are analyzed as follows:

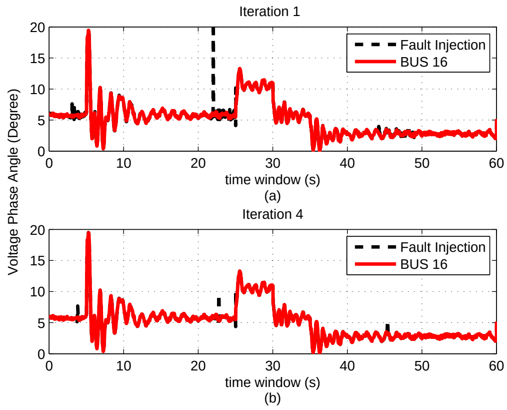

Fig. 5. Performance of proposed method at different iterations at Bus 16

The first injection scenario consisted of a few large spikes spread across two monitoring windows. As a result, the accuracy of 5-10 and 10-15 second windows are impacted. Since the larger spike as well as the three-phase-to-ground fault occurred in the 5-10 second period, both methods incurred their highest MSE values. However, the proposed scheme is still able to provide oscillatory parameters with adequate precision whereas the distributed method failed to track one electromechanical mode. This is due to initial estimates collected from the interaction of neighboring sensors.

In the second injection scenario, the system contained less non-linear dynamics and oscillations are more dominant in measurements. Here, the largest spike was introduced during the 20 to 25 second window, which has caused the distributed scheme to fail to track one oscillation. Although high energy signals were injected, they did not flood the entire monitoring window. Hence, the distributed scheme managed to track all three oscillations in the following time window. Nevertheless, the lowest frequency mode (0.69 Hz) incurred noticeable estimation errors. For the proposed TFMP, the removal of abnormal data segments through subsystem diagonalization helps to avoid them from incurring errors into the estimation stage. As a result, the proposed scheme maintained similar estimation accuracy as in the case of without data-injections.

Next, the third injection scenario is examined. Since the injected measurements from Bus 16 and 17 contained amplitudes and characteristics similar to collected synchrophasor measurements, extracting oscillatory parameters is more challenging than previous scenarios. This can be reflected by the consecutive high MSE values generated by both methods during the time of 40 to 50 seconds. The filtering stage of the distributed method was not able to remove injected data, which caused it to lose track of one oscillatory mode due to slow convergence of EM. In contrast, the proposed TFMP estimation scheme still computed accurate oscillation parameters. An interesting ob-

TABLE I

TEST CASE I – NEW ENGLAND SYSTEM: DETECTING MULTIPLE OSCILLATIONS IN THE PRESENCE OF RANDOM DATA-INJECTION ATTACKS[1]

Measurements	ζ_D	f_D	ζ_{TFMP}	f_{TFMP}	ζ_D	f_D	ζ_{TFMP}	f_{TFMP}	ζ_D	f_D	ζ_{TFMP}	f_{TFMP}	ζ_D	f_D	ζ_{TFMP}	f_{TFMP}
Time	**0 s–5 s**				**5 s–10 s**				**10 s–15 s**				**15 s–20 s**			
	4.1 6.0 5.8	0.69 1.07 1.12	3.7 5.9 5.7	0.69 1.07 1.13	3.9 – 5.4	0.73 – 1.17	3.8 5.9 5.5	0.70 1.05 1.17	4.0 5.5 5.4	0.69 1.12 1.17	3.8 5.7 5.6	0.69 1.12 1.17	4.2 5.9 5.7	0.68 1.07 1.11	3.9 5.9 5.8	0.69 1.07 1.12
MSE	2.1×10^{-2}		1.8×10^{-3}		5.5×10^{-1}		4.8×10^{-2}		2.5×10^{-2}		3.1×10^{-3}		2.2×10^{-2}		2.1×10^{-3}	
Time	**20 s–25 s**				**25 s–30 s**				**30 s–35 s**				**35 s–40 s**			
	3.9 5.8 –	0.71 1.11 –	3.9 5.6 5.6	0.69 1.11 1.17	4.0 5.9 5.7	0.72 1.07 1.12	3.9 5.9 5.7	0.68 1.07 1.14	4.3 5.7 5.2	0.69 1.08 1.12	3.9 5.8 5.7	0.69 1.08 1.13	4.0 5.6 5.5	0.69 1.11 1.15	3.9 5.6 5.5	0.69 1.11 1.16
MSE	2.1×10^{-1}		2.4×10^{-3}		4.2×10^{-1}		3.6×10^{-3}		5.5×10^{-2}		2.5×10^{-3}		4.5×10^{-2}		3.9×10^{-3}	
Time	**40 s–45 s**				**45 s–50 s**				**50 s–55 s**				**55 s–60 s**			
	4.3 – 5.2	0.70 – 1.14	3.9 5.6 5.6	0.69 1.11 1.15	4.3 – 5.8	0.69 – 1.14	3.9 5.8 5.7	0.70 1.10 1.14	4.5 5.7 5.9	0.66 1.13 1.00	3.9 5.9 5.7	0.69 1.09 1.14	4.4 – 5.1	0.69 – 1.11	3.9 5.6 5.6	0.69 1.11 1.17
MSE	8.3×10^{-1}		6.8×10^{-3}		6.5×10^{-1}		5.7×10^{-3}		2.2×10^{-1}		1.9×10^{-3}		9.8×10^{-1}		2.7×10^{-3}	

[1] In this table, ζ is the damping ratio i.e. $\zeta = \frac{-\sigma}{\sqrt{\sigma^2+(2\pi f)^2}} \times 100$. f is the frequency in hertz, MSE is the mean-square error, subscript D and TFMP are the acronyms of Distributed approach [18] and the proposed TFMP, respectively.

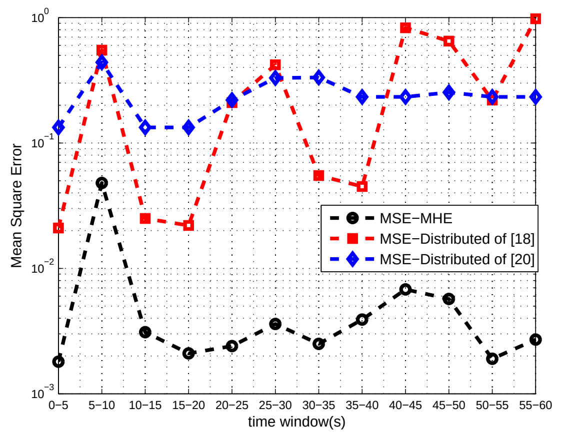

Fig. 6. Estimation comparison analysis of different methods at Bus 16

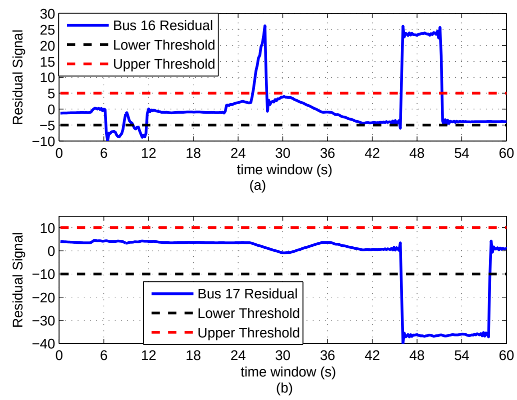

Fig. 7. Fault residual evaluation in a) Bus 16, and b) Bus 17

servation is made during the sole injection of ambient data at Bus 17 throughout the entire 50-55 second window. Despite the distributed method from [18] has detected all three oscillations, the frequency and associated damping factor of the inter-area oscillation (0.69 Hz mode) incurred most errors compared with all other windows. The estimated incorrect higher damping ratio can delay subsequent damping strategies, and reduce the effectiveness of the system damping capability. As a result, a cascading failure leading to wide-area blackouts can potentially occur at a later stage. In comparison, the proposed TFMP estimation is able to mitigate such abnormalities and maintained reasonable estimation accuracy for all oscillatory modes. The removals of ambient grid-like dynamics are illustrated in Fig.5 for Bus 16. Referring to these plots, the proposed scheme iteratively minimize data abnormalities by removing them as outliers using the derived cross-covariance relationships.

Finally, the fourth injection scenario is presented. There is a more realistic and challenging scenario to mitigate the previous events. During the attack at Bus 16 from 44-49 seconds, both schemes performed well due to their property of retrieving missing measurements to make an accurate estimation of oscillations. However, during the data-repetition attack at Bus 17 from 55-60 second window, the distributed scheme of [18] was unable to predict the model and tackle the noise variances independently. This resulted in a high MSE value generated by the distributed algorithm. Moreover, the algorithm is also not able to track one of the nearby oscillation modes. In contrast, the proposed TFMP scheme estimated all oscillations accurately. The incorporation of the model prediction demonstrates that using MHE and calculating the covariances of each local sensor helps to achieve better MSE values. To observe the impact of Bus 16 during all these data-injections, an MSE based comparison has been made between the proposed TFMP scheme, the distributed scheme of [18], and the distributed scheme proposed of [20]. Results are shown in Fig. 6, where all three schemes performed reasonably well. However, if the level of precision is considered, the proposed TFMP supersede the other two schemes especially when estimating the oscillatory modes between 40 to 60 seconds.

Once the estimation accuracy is achieved, the residuals are generated to quantify any system variations. Referring to Fig. 7, all attacks have been detected using the threshold selection by a coherence function. The threshold selected for Bus 16 and Bus 17 residuals are ± 5 and ± 10, respectively using the coherence spectrum function. As observed in Fig. 7(a), some wiggles within the threshold limits correspond to the dynamics of real-time system. However, they can also be mistaken as system faults if inappropriate thresholds are selected. In this case, the threshold selection algorithm is adequate to detect the system faults while avoiding the false alarms. Overall, residuals exceeded the thresholds coincide with the time of data-injection events. Meanwhile, the residual profile of Bus 17 shows less variations as observed in Fig. 7(b). This is because the location has been subjected to less data-injection attacks than Bus 16. Nevertheless, the more challenging data-repetition attack has been well-detected by the coherence function-based threshold.

IV. Conclusions

In this paper, the proposed TFMP based monitoring scheme is proposed and demonstrated to estimate power oscillations modes during data-injection attacks. The model prediction property of the algorithm has helped to remove bias and noise while accurately extracting the system parameters. It is further facilitated by the derived diagonalized interaction filter, which tackles the error covariance in the form of subsystems, and thus improving the initial oscillatory state estimates. As a result, the incorporation of the proposed algorithm into oscillation detection has provided more accurate results than existing oscillation monitoring schemes in the presence of data-injection attacks. The immunity of monitoring applications against intentional data-injections has been enhanced. In the future, studies to quantitatively verify the effectiveness and robustness of the proposed method to more adverse non-regional threats will be conducted.

Appendix

A. Computation of Matrix weights for (12) to (14)

The matric weights have been computed by taking inverse of (1) to (2) using linear minimum variance [23]. It is as follows: $\kappa_0 = \alpha_1^{-1}\Psi_1$, $\Psi_0 = \alpha_1^{-1}\Psi_1$, $\bar{H}_t^i = H_{1,t}^i + H_{2,t}^i\bar{\kappa}$, $\bar{v}_t^i = \Psi_3^i w_t + v_t^i$, $\Psi_3^i = H_{2,t}^i\bar{\Psi}$, $\bar{\kappa} = \kappa_3^{-1}\alpha_2\alpha_1^{-1}\kappa_1 - \kappa_3^{-1}\kappa_2$, $\bar{\Psi} = \kappa_3^{-1}\alpha_2\alpha_1^{-1}\Psi_1 - \kappa_3^{-1}\Psi_2$.

References

[1] S. Gorman, "Electricity grid in U.S. penetrated by spies," *Wall St. J.,*, PP. A1, Apr. 6, 2009.

[2] L. C. Baldor, "New Threat: Hackers look to take over power plants," *IEEE Trans. Power Syst.*, Aug. 3, 2010 [Online], Available: http://abcnews.go.com/Business/wireStory?id=11316203.

[3] T. T. Kim, H. V. Poor, "Strategic protection against data-injection attacks on power grids," *IEEE Trans. Power Syst.*, vol. 2, no. 2, pp. 326–333, June 2011.

[4] 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.

[5] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," *IEEE J. Sel. Areas Comm.*, vol. 31, no. 7, pp. 1306–1318, Jul 2013.

[6] O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *IEEE J. Sel. Areas Comm.* vol. 30, no. 6, pp. 1108–1118, Jul 2012.

[7] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. of IEEE*, vol. 100, pp. 210–224, 2012.

[8] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, pp. 645–658, 2011.

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

[10] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, pp. 659-666, 2011.

[11] P. Kundur, N. J. Balu, and M. G. Lauby, "Power system stability and control," *McGraw-hill New York*, vol. 7, 1994.

[12] G. Rogers, "Power system oscillations," *Kluwer Academic Boston*, 2000.

[13] A. Messina, "Inter-area oscillations in power systems: A nonlinear and nonstationary perspective," *Springer*, 2009.

[14] J. J. Sanchez-Gasca, and J. H. Chow, "Performance comparison of three identification methods for the analysis of electromechanical oscillations," *IEEE Trans. Pow. Syst.*, vol. 14, no. 3, pp. 995–1001, Aug. 1999.

[15] S. A. N. Sarmadi, and V. Venkatasubramanian, "Electromechanical mode estimation using recursive adaptive stoachastic subspace identification," *IEEE Trans. Pow. Syst.*, vol. 29, no. 1, pp. 349–358, Jan 2014.

[16] R. W. Wies and J. W. Pierre, "Use of least-mean square (LMS) adaptive filtering technique for estimating low-frequency electromechanical modes of power systems," *Proc. Amer. Ctrl. Conf.*, vol. 6, pp. 4867–4873, May 2002.

[17] J. C.-H. Peng and N. C. Nair, "Enhancing Kalman filter for tracking ringdown electromechanical oscillations," *IEEE Trans. Pow. Syst.*, vol. 27, no. 2, pp. 1042–1050, 2012.

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

[19] D. N. Kosterev, C. W. Taylor, and W. A. Mittelstadt, "Model validation for the August 10, 1996 WSCC system outage," *IEEE Trans. Pow. Syst.*, vol. 14, no. 3, pp. 967–979, Aug. 2002.

[20] L. Xie, D. -H. Choi, S. Kar, and H. V. Poor, "Fully distrubted state estimation for wide-area monitoring systems," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1154–1169, Sep 2012.

[21] H. Mitchell, "Multi-sensor data fusion: An introduction," *NewYork: Springer*, 2007.

[22] V. L. Syrmos, F. L. Lewis, "Robust eigenvalue assignment for generalized systems, " *Automatica*, vol. 28, no. 5, pp. 1223–1228, 1992.

[23] U. Shaked and C. E. de Souza, "Robust minimum variane filtering," *IEEE Trans. Sig. Process.*, vol. 43, no. 11, pp. 2474–2483, November 1995.

[24] Z. L. Deng, "Kalman filtering and Weiner filtering - Modern time series analysis method," *Harbin: Harbin Inst. of Tech.*, pp. 1–396, 2001.

[25] T. Yanagisawa, H. Takayama, "Coherence coefficient measuring system and its application to some acoustic measurements", *Appl. Acoustics*, vol. 16, no. 2, pp. 105–119, Mar. 1983.

[26] C. Zheng, H. Yang, and X. Li, "On generalized auto-spectral coherence function and its applications to signal detection", *IEEE Sig. Process. letters*, vol. 21, no. 5, pp. 559–563, May 2014.

[27] B. Pal and B. Chaudhuri, Robust control in power systems: *Springer*, 2005.

[28] J. C.-H. Peng and J. L. Kirtley, "An improved empirical mode decomposition method for monitoring electromechanical oscillations," *IEEE PES Inn. Smart Grid Techn. Conf. (ISGT)*, pp. 1-5, 2014.

[29] DIgSILENT, "PowerFactory 15 user manual," 2013.

Haris M. Khalid (M'13) received his M.S and Ph.D. degrees 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 at Distributed Control Research Group at KFUPM. Since 2013, he has been working as a Postdoctoral Researcher with Department of Electrical Engineering and Computer Science at Masdar Institute of Science and Technology (MI) collaborated with MI-MIT Cooperative Program. His research interests are power systems, signal processing, 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. In 2012, he joined the Department of Electrical Engineering and Computer Science at Masdar Institute of Science and Technology, Abu Dhabi, United Arab Emirates, as an Assistant Professor of Electrical Power Engineering. He was a Visiting Scientist with the Research Laboratory of Electronics (RLE) and a Visiting Assistant Professor with the MIT-MI Cooperative Program at Massachusetts Institute of Technology (MIT), in 2013 and 2014, respectively. His research interests are power system stability, synchrophasor measurements, real-time system identification, and high performance computing.