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 address 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 systems 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 inter-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-
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 cyberattacks 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 computationally 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 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 (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 − 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. \( x_{1,t} \), \( H_{1,t} \), \( z_{1,t} \)).
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 expressed as:

\[ \alpha x_{t+1} = f(x_t, w_t), \quad t = 0, 1, \ldots, T \]

where \( \alpha \) is the constant matrix with compatible dimensions to the model dynamics, \( f(\cdot) \) is the nonlinear function representing the state transition model, \( x_0 \in \mathbb{R}^n \) is the initial condition of the oscillation state, superscript \( r \) is the size of the oscillation state vector in the subspace \( \mathbb{R}^r \). In addition, \( w_t \in \mathbb{R}^r \) 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:

\[ z_i^t = h_i(x_t) + v_i^t, \quad i = 1, \ldots, N \]

where \( z_i^t \in \mathbb{R}^{p_i} \), \( p_i \) is the number of synchrophasor observations made by the \( i \)-sensor, \( (\cdot)_i \) is a nonlinear function representing the local observation matrix of \( i \)-th sensor, \( x_t \) is the state matrix for oscillations, and \( v_i^t \in \mathbb{R}^{p_i} \) is the observation noise of the \( i \)-th sensor. A dynamical power grid will be governed by the following constraints:

\[ x_t = X_t, \quad w_t \in W_t, \quad v_t \in V_t \]

where \( X_t, V_t \) and \( W_t \) are assumed to have Gaussian probability distribution function.

Assumption II.1: The noises \( w_t \) and \( v_t \) are all initially assumed to be uncorrelated zero-mean white Gaussian such that 

\[ E[w_t] = E[v_t] = 0, \quad \forall t. \]

Note \( E \) denotes the expectation operator, and superscript * denotes the transpose operator. Also, 

\[ E[w_t w_t^*] = R_t \delta_{gh}, \quad E[v_t v_t^*] = Q_t \delta_{gh}, \quad \forall t, \]

where \( R_t \) represents the residual covariance, \( \delta_{gh} \) 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 \( K \) num-
umber of electromechanical oscillations. Referring to (2), the observation output signal \( z_i^t \) from an \( i \)-th sensor at time \( t \) can be modeled in the frequency domain as:

\[
z_i^t = \sum_{k=1}^{K} a_k e^{(-\sigma_k + j2\pi f_k)T_s} + v_i^t, \quad t = 1, 2, \ldots, T \tag{4}
\]

where \( a_k \) is the complex amplitude of \( k \)-th mode, \( \sigma_k \) 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. the linearized model of the system 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:

\[
f_i^t(x_i, w_i) \approx f_i^t(\tilde{x}_i^t(0) + \kappa_i(x_i - \tilde{x}_i^t(0)) + \Psi_i w_i \tag{6}
\]

\[
h_i^t(x_i) \approx h_i^t(\tilde{x}_i^t(0) + H_i^t(x_i - \tilde{x}_i^t(0)) \tag{7}
\]

where \( \kappa, \Psi \), and \( H^t \) are the Jacobian matrices with compatible dimensions used to linearize the nonlinear dynamics:

\[
\kappa_i = \frac{\partial f_i(x, 0)}{\partial x}\bigg|_{x=\tilde{x}_i^t(0)}, \Psi_i = \frac{\partial f_i(\tilde{x}_i^t(0), w)}{\partial w}\bigg|_{w=0}, \tag{8}
\]

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

\[
\alpha x_{i,t+1} = \kappa x_i + \Psi w_i \tag{9}
\]

\[
z_i^t = H^t x_i + v_i^t, \quad i = 1, 2, \ldots, N \tag{10}
\]

where the oscillation system state \( x_i \in \mathbb{R}^n \), the synchrophasor measurements \( z_i^t \in \mathbb{R}^{n_i}, w_i \in \mathbb{R}^r \), and \( v_i^t \in \mathbb{R}^{n_i} \). Variables \( \alpha, \kappa, \Psi, \) and \( H^t \) are the constant matrices with compatible dimensions. The system model described by (9) and (10) is derived based on the following assumptions:

- \( \text{rank } \alpha = n_1 < n, \text{ and } \text{rank } \kappa \geq n_2, \) where \( n_1 + n_2 = n \).
- System (9) is regular, i.e. \( \det(\alpha - \kappa) \neq 0 \), where \( \alpha \) is an arbitrary complex number which can be expressed as a sum of real and imaginary components.
- The initial state \( x_{0} \), with mean \( \mu_0 \) and variance \( P_0 \), is independent of \( w_i^t \) and \( v_i^t \).

1) Diagonlization of the System Model at Node \( i \) into Subsys-tems:

Accurate monitoring of power oscillations in the presence of data-injection attacks can prove to be computationally expensive. However, to tackle the additional computational cost due to the calculation of initial estimates and the error covariance matrix \( P_{i,t-1} \) 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 KLFP-based smoother which can be referred to (19)-(26) in [18]. In [18], the KLFP-based smoother \( \tilde{x}_{i,t|0}^\kappa \) of the state \( x_i \) is calculated based on measurements \( z_i^t, \ldots, z_i^{T-1} \). Note the attacked system at node \( i \) can be diagonalized up to \( N \) number of subsystems. To simplify the formulation, diagonal-ization 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:

\[
L = [\alpha_1 \ 0 \ \alpha_2 \ 0], \ LkR = [\kappa_1 \ 0 \ \kappa_2 \ k_3], \ L\Psi R = [\Psi_1 \ \Psi_2 \ H^t R = [H_1^t \ H_2^t] \tag{11}
\]

where \( \alpha_1 \in \mathbb{R}^{n_1 \times n_2} \) is non-singular lower-triangular, \( \kappa_1 \in \mathbb{R}^{n_1 \times n_1} \) is quasi-lower-triangular, \( \kappa_3 \in \mathbb{R}^{n_2 \times n_1} \) is non-singular lower-triangular. Transforming \( x_i = R[x_{i,t} \ x_{i,t}^t] \), where \( x_{i,t} \in \mathbb{R}^{n_1}, x_{i,t}^t \in \mathbb{R}^{n_2} \). 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 mini-
mum variance [23]:

\[
x_{1,t+1} = \kappa_0 x_{1,t} + \Psi_0 w_t
\]

\[
x_{2,t} = \kappa x_{1,t} + \Psi v_t
\]

\[
z_t^i = \hat{H}^i_{1} x_{1,t} + \omega_t^i
\]

where \(x_{1,t}\) and \(x_{2,t}\) are the states of subsystem 1 and subsystem 2, respectively. \(\kappa_0, \Psi_0, \kappa, \Psi, \hat{H}\) and \(\omega\) are diagonalized variables, which are computed from the inverse of weighted matrices \(\alpha_i\) and \(\kappa_3\) 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 \(\bar{v}_t\) and \(\bar{v}_t\) will have the diagonalizable expected value:

\[
E\left[ \begin{bmatrix} \bar{v}_t^1 \\ \bar{v}_t^2 \end{bmatrix} \right] = Q_t^{1/2} \sigma_t^{1/2}
\]

where \(Q_t^{1/2}\) is the process noise correlation factor between subsystem 1 and 2, \(\sigma_t^{1/2}\) 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:

\[
Q_t^{1/2} = \begin{bmatrix} Q_\psi & \alpha^2 \\ \alpha^* & Q_{\psi}^{-1} \end{bmatrix}
\]

where \(\alpha = Q_\psi \Psi_0^*, \omega = \Psi_0 Q_\omega \Psi_0^* + Q_\omega\) and \(Q_{\psi}^{1/2} = \Psi_0 Q_\psi^{1/2} Q_\omega^{1/2}\) 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:

\[
\tilde{x}_{1,t+1} = \tilde{\kappa}_0 (I_n - \beta^2 t^i \hat{H}^i_t) \tilde{x}_{1,t} + \Psi_0 w_t - \left( \tilde{\kappa}_0^2 \beta^2_t + J^i \right) \bar{v}_t^i
\]

where \(\tilde{x}_{1,t+1}\) is the difference between \(x_{1,t}\) and \(x_{1,t+1}\), \(\tilde{\kappa}_0 = \kappa_0 - J^i \hat{H}^i_t, J^i = \Psi_0 \alpha^2 Q_\omega^{-1}, \tilde{\kappa}^i = \kappa (I_n - \beta^2 t^i \hat{H}^i_t) - \Psi_0 \alpha^2 Q_\omega^{-1} \hat{H}^i_t, I_n\) is an \(n\times n\) identity matrix. For notation convenience, \(\beta^2_t = \frac{F_t^i}{J^i + \hat{H}^i_t}\). The corresponding updated a-posteriori equation of state \(x_{1,t}\) at node \(i\) will be:

\[
\tilde{x}_{1,t} = \tilde{\kappa}_0 (I_n - \beta^2 t^i \hat{H}^i_t) \tilde{x}_{1,t+1} - \beta^2 t^i \bar{v}_t^i
\]

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

\[
\tilde{x}_{2,t} = F_t^i \tilde{x}_{1,t} + D_t^i \bar{v}_t^i
\]

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

\[
\tilde{x}_{2,t}^i = F_t^i \tilde{x}_{1,t} + D_t^i \bar{v}_t^i
\]

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

\[
\tilde{x}_{2,t}^i = F_t^i \tilde{x}_{1,t} + D_t^i \bar{v}_t^i
\]

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

\[
\tilde{x}_{2,t}^i = F_t^i \tilde{x}_{1,t} + D_t^i \bar{v}_t^i
\]

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

\[
\tilde{x}_{2,t}^i = F_t^i \tilde{x}_{1,t} + D_t^i \bar{v}_t^i
\]

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

\[
\tilde{x}_{2,t}^i = F_t^i \tilde{x}_{1,t} + D_t^i \bar{v}_t^i
\]

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

\[
\tilde{x}_{2,t}^i = F_t^i \tilde{x}_{1,t} + D_t^i \bar{v}_t^i
\]

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

\[
\tilde{x}_{2,t}^i = F_t^i \tilde{x}_{1,t} + D_t^i \bar{v}_t^i
\]
smoothed run:

\[ P_{\nu_{1,\tau}}^{S_{1,2}} + \rho_{\text{track fusion}}^{y_{1,\tau}} (I_n - \beta_2 H^2) ] + P_{\nu_{1,\tau}}^{S_{1,2}} (I_n - \beta_2 H^2) \]

\[ + H^2 \{ H^2 P_{\nu_{1,\tau}} H^2 + \rho_{\text{track fusion}}^{y_{1,\tau}} \}^{-1} H^2 \]  

(26)

The derived cross-covariance for smoothing the state \( x_{t_1} \) between subsystem 1 and 2 are:

\[ P_{\nu_{1,\tau}}^{S_{1,2}} (I_n - \beta_2 H^2) = (H^2 P_{\nu_{1,\tau}} H^2 + \rho_{\text{track fusion}}^{y_{1,\tau}})^{-1} \]

(27)

\[ P_{\nu_{2,\tau}}^{S_{1,2}} (I_n - \beta_2 H^2) = (H^2 P_{\nu_{1,\tau}} H^2 + \rho_{\text{track fusion}}^{y_{1,\tau}})^{-1} \]

(28)

where \( P_{\nu_{1,\tau}}^{S_{1,2}} \) and \( P_{\nu_{2,\tau}}^{S_{1,2}} \) are the smoothing error covariance of state \( x_{t_1} \) and \( x_{t_2} \) 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 can be determined.

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

Based on (12)-(14) for subsystem 1 and 2, the interaction filter can be stated for state \( x_{t_1} \) of subsystem 1 as:

\[ \tilde{x}_{1,t}^{\text{P}} = (e_1^2 T_{1,t} e_2) \]  

where superscript \( \text{P} \) denotes the interaction between subsystem 1 and 2. \( e_1, t \) is an \( n_1 \times n_1 \) matrix, \( y_{1,t} = P_{1,2}^{y_{1,\tau}} \) is an \( n_2N \times n_2 \) matrix. Vectors of \( \tilde{x}_{1,t}^{\text{P}} \) and \( \tilde{x}_{2,t}^{\text{P}} \) are given by:

\[ P_{\nu_{1,\tau}}^{S_{1,2}} (I_n - \beta_2 H^2) = (H^2 P_{\nu_{1,\tau}} H^2 + \rho_{\text{track fusion}}^{y_{1,\tau}}) \]

(29)

(30)

Restoring the variance of (12)-(14) to the main singular system described by (9) and (10) made the filter into:

\[ \tilde{x}_{1,t}^{\text{P}} = R [ \tilde{x}_{1,t}^{\text{P}} \tilde{x}_{2,t}^{\text{P}} ] \]

(32)

The variance of the filtering error of \( \tilde{x}_{1,t}^{\text{P}} \) in (32) can be computed by:

\[ P_{\nu_{1,\tau}}^{S_{1,2}} = R \left[ \begin{array}{cc} P_{1,2}^{y_{1,\tau}} & P_{1,2}^{y_{1,\tau}} \end{array} \right] \]

(33)

where covariance matrix \( P_{1,2}^{y_{1,\tau}} \) and \( P_{1,2}^{y_{1,\tau}} \) are computed by (21) and (22), respectively. The covariance matrix \( P_{\nu_{1,\tau}}^{S_{1,2}} \) between filtering errors \( \tilde{x}_{1,t}^{\text{P}} \) and \( \tilde{x}_{2,t}^{\text{P}} \) can then be defined as:

\[ P_{\nu_{1,\tau}}^{S_{1,2}} = P_{\nu_{1,\tau}}^{S_{1,2}} (I_n - \beta_2 H^2) \]

(34)

where \( P_{\nu_{1,\tau}}^{S_{1,2}} = P_{\nu_{1,\tau}}^{S_{1,2}} \) and \( P_{\nu_{1,\tau}}^{S_{1,2}} = P_{\nu_{1,\tau}}^{S_{1,2}} \) can be computed as follows:

\[ P_{\nu_{1,\tau}}^{S_{1,2}} = (I_n - \beta_2 H^2) \]

(35)

where \( P_{\nu_{1,\tau}}^{S_{1,2}} = P_{\nu_{1,\tau}}^{S_{1,2}} \). Likewise, the variance of smoothing error of \( \tilde{x}_{1,t}^{\text{P}} \) 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 \((z_1, \ldots, z_{\tau})\) at time \( t \), the MAP criteria for calculating the oscillation estimate with constraints can be expressed as:

\[ x_{1,t}^{\text{MAP}} = \arg \max_{x_{1,t} \in \mathbb{T}} p(x_{1,t} \mid x_{1,\tau} \mid z_{1,\tau}) \]

(36)

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

\[ \log p(x_{1,t} \mid z_{1,\tau}) = \sum_{t=0}^{T-1} \left[ \vert x_{1,t} - \Theta(x_{1,t}) \right] \]

(37)

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

\[ \min_{w_{1,t}, \ldots, w_{1,T}} \sum_{t=0}^{T-1} L_t(w_{1,t}, \ldots, w_{1,T}) \]

(38)

where \( L_t \) and \( \Theta \) are positive functions, and \( L_t(w_{1,t}, \ldots, w_{1,T}) = \sum_{t=0}^{T-1} \left[ \vert x_{1,t} - \Theta(x_{1,t}) \right] \). 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 \( z_{1,T}^{\text{TF}} \). The superscript TF denotes the track fusion, and \( z_{1,T}^{\text{TF}} \) 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:

\[ z_{1,T}^{\text{TF}} = H_{1,T}^T x_{1,t} + w_{1,T}^{\text{TF}} \]

(39)

Similar to (2), the corresponding observation model is \( H_{1,T}^T \), and the noise vector is \( w_{1,T}^{\text{TF}} \). They can also be expressed as an array of information collected from all substations as \( z_{1,T}^{\text{TF}} \).

\[ H_{1,T}^T = [H_{1,1}, \ldots, H_{1,N}]^T \]

(40)

where \( N \) is the number of sensors. Considering the track estimation-based variables \( z_{1,T}^{\text{TF}}, H_{1,T}^T \), and \( w_{1,T}^{\text{TF}} \), the oscillation state estimate at TFC can be presented as:

\[ x_{1,t}^{\text{TF}} = [H_{1,T}^T]^{-1} [H_{1,T}^T x_{1,t} + w_{1,T}^{\text{TF}}] \]

(41)
where $P^{T}_{i,t} = [\sum_{i=1}^{N} P^{T}_{i,t}]^{-1}$. 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:

$$P^{ij}_{i,t} = E[x^{ij}_{i,t}x^{ij \dagger}_{i,t}] = [1 - w_{i}P^{ij}_{i,t-1}]$$

where $x^{ij}_{i,t} = x_{i,t} - x_{i,t}$. This is derived based on the same principles as the covariance of the subsystems within one monitoring node. Hence, $P^{ij}_{i,t}$ 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 $x_{1,t}, x_{2,t} \in \mathbb{R}^{n}$, 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 $H_{t}[s\,\mathbb{I} - (\kappa_{t} - K_{t}H_{t})^{-1}]$ is strictly positive real, where $K_{t} \in \mathbb{R}^{m \times n}$ is chosen such that $A_{t} - K_{t}H_{t}$ is stable. Thus, the following expression is constructed as:

$$\hat{x}_{t} = \kappa\hat{x}_{t} + (u_{t}, z_{t}) + \xi_{f,t}(u_{t}, z_{t}, \hat{x}_{t}) + K_{t}(z_{t} - \hat{z}_{t})$$

where $\xi_{f} \in \mathbb{R}$ 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 $(\kappa_{t}, H_{t})$ is assumed to be observable, $K_{t}$ can be selected to ensure $\kappa_{t} - K_{t}H_{t}$ is a stable matrix. This can be defined as:

$$e_{x,t} = x_{t} - \hat{x}_{t}, \quad e_{z,t} = z_{t} - \hat{z}_{t}$$

Error equations will then become:

$$e_{x,t+1} = (\kappa_{t} - K_{t}H_{t})e_{x,t} + [\xi_{t}(u_{t}, z_{t}, x_{t}) - \xi_{f,t}(u_{t}, z_{t}, \hat{x}_{t})]$$

$$e_{z,t} = H_{t}e_{x,t}$$

Once 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 $\omega$ is the frequency in rad/s. The magnitude-squared coherence spectrum of the two signals can be defined as:

$$c(\hat{G}(\omega), \hat{G}_{f}(\omega)) = \frac{|\hat{G}(\omega)\hat{G}_{f}(\omega)|^{2}}{|\hat{G}(\omega)|^{2}||\hat{G}_{f}(\omega)|^{2}}$$

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:

$$test_{stat} = \begin{cases} \leq th \forall \theta \in \Omega & fault \\ > th \forall \theta \in \Omega & no \ fault \end{cases}$$

where $0 \leq th \leq 1$ is a threshold value. $\Omega$ 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. Modelling details are based on [27, 28]. In this study, synchrophasor measurements are collected from Bus 15, 16, 17, 24, 30, 35, 37, 38, and 39. From these data, three dominant electromagnetic 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 DlgsILENT 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 electromagnetic 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.
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 seconds. 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:

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

<table>
<thead>
<tr>
<th>Measurements</th>
<th>0 s–5 s</th>
<th>5 s–10 s</th>
<th>10 s–15 s</th>
<th>15 s–20 s</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSE−MHE</td>
<td>4.1</td>
<td>6.0</td>
<td>5.8</td>
<td>5.2</td>
</tr>
<tr>
<td>MSE−Distributed of [18]</td>
<td>3.9</td>
<td>5.9</td>
<td>5.6</td>
<td>5.2</td>
</tr>
<tr>
<td>MSE−Distributed of [20]</td>
<td>3.9</td>
<td>5.9</td>
<td>5.6</td>
<td>5.2</td>
</tr>
</tbody>
</table>

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

![Fig. 6](image)

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

![Fig. 7](image)

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.

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 variences indepen-

![Table I](image)
faults while avoiding the false alarms. Overall, residuals exceed 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 matrix weights have been computed by taking inverse of (1) to (2) using linear minimum variance [23]. It is as follows:

\[ \kappa_i = \alpha_1^{i-1} \Psi_1, \quad \varrho_i = \alpha_1^{i-1} \Psi_2, \quad H_1^i = H_1^{i-1} + H_2^{i-1} \kappa, \]
\[ \gamma_i = \Psi_3^{i-1} \varrho_i + \kappa_i, \quad \Psi_4^i = H_2^{i-1} \gamma_i, \quad \psi_i = \kappa_i^{i-1} \alpha_1^{i-1} \psi_1 - \kappa_i^{i-1} \psi_2. \]

REFERENCES