A Prediction Algorithm to Enhance Grid Resilience towards Cyber Attacks in WAMCS Applications

Ahmed S. Musleh, *Student Member, IEEE,* Haris M. Khalid, *Member, IEEE,*
S. M. Muyeen, *Senior Member, IEEE,* and Ahmed Al-Durra, *Senior Member, IEEE*

***Abstract*— Monitoring and control of electrical power grids are highly reliant on the accuracy of the digital measurements. These digital measurements reflect the precision of the installed sensors which are vulnerable to the injection of unknown parameters in the form of device malfunction and cyber-attacks. This may question the operational security and reliability of many cyber-physical infrastructure such as smart grid. To resolve this issue, a multi-sensor temporal prediction based wide-area control (TPWAC) scheme is proposed in this paper. The feasibility of the designed scheme is verified in an advanced synchrophasor measurements based wide-area monitoring and control system (WAMCS). This WAMCS adopts a flexible AC transmission system (FACTS) device (the primary controller) for controlling the smart grid's voltage profile. The algorithm is validated in a real-time environment with an innovative software-in-the-loop (SIL) testing setup. The performance of the proposed technique in the presence of false data injection attacks shows promising results.**

***Index Terms*—Cyber-physical systems, cyber security, distributed Kalman filter, false data-injection attack, flexible AC transmission system (FACTS), phasor measurement unit (PMU), real time digital simulator (RTDS), smart grid, wide-area monitoring and control system (WAMCS).**

I. Introduction

DUE to the emergence of the additional power sources and loads, reliability and security are among the most significant concerns to be considered in smart grids nowadays [1]. These additional elements have the property to add pressure on power grid operations which may lead to frequency deviations and voltage instability. Consequently, the situational awareness of power grid has been enhanced by introducing wide-area monitoring and control systems (WAMCS), which provided an advanced visualization and control of the grid parameters. Among WAMCS applications in smart grid, voltage control is identified as one of the most important schemes [2]. This scheme is distinct in literature as the secondary voltage control method (SVCM), which is a managerial control loop that assigns dissimilar set-points for various reactive power components employed for reducing voltage profile deviations in smart grid [3]. The importance of this scheme is reinforced following the August 14^{th}, 2003 Northeast blackout, where it was recognized that WAMCS could have helped to identify and prevent this major voltage collapse [4]. The main profit of SVCM scheme is improving the stability margin of the grid by reducing the total voltage deviations [5]. SVCM has been explored widely over the last few years. In [6], a straightforward approach to automatic voltage control is considered where an optimization problem is formulated for SVCM. Authors of [6, 7] proposed an adaptive SVCM where learning process and multiple optimization problems are discussed. In [8], the employment of model predictive control (MPC) in SVCM is deliberated where different cases are studied and examined confirming a decent performance of the suggested algorithm. Engagement of multi-agent Systems (MAS) is presented in [9] where various agents' organizations are built and compared. The majority of studies conducted on WAMCS are based on the speculation of having full wide-area measurements, which is not applicable; still, some authors have debated the use of phasor measurement units (PMU) for data collections.

PMU applications in power systems have grown significantly over the past few years [10]. Nowadays, PMUs are seen as the foundation of WAMCS applications [11]. They provide much improved grid-wide measurements compared to the asynchronous and slow pace of measurements collected via classic SCADA systems; this is due to the employment of the delicate timestamp via the global positioning system (GPS) and the advanced information technology infrastructure [12]. However, the dependency of WAMCS on digitalized tools such as PMUs unleashes a huge set of threats of cyber-attacks [13, 14]. Threats are more evident when grid-wide control actions are based on the measurements collected from those digital tools. The main impact of cyber threats emerged from this perspective [15, 16]. In [17], the authors illustrate how disastrous the economic impact of malicious data attacks on the grids' market operations could be. In 2016, a major cyber-attack took place in Ukraine resulting in knocking out 200 Megawatts, which is about 20% of the Kievs night-time energy consumption [18]. This incident emphasized the importance of protection schemes against such threats.

Conventional bad-data (false-data) protection techniques are based on the classical weighted least-square estimation where redundancy is a must in detecting the bad-data [19]. On the other hand, advanced detection techniques adopted different approaches. For instance, three interleaved hop-by-hop authentication schemes are presented in [20] to detect injected false dataand discard it. Machine-learning based bad-data detection algorithms have been introduced in [21] where two methods are developed using supervised and unsupervised learning. Authors of [22] proposed a novel bad data detection algorithm that requires sensors to do a lightweight computation and report statistical data in addition to the current readings. Bad-data detection via Kalman filtering has been investigated in [23], where the Euclidean detector is employed in the detection process. A dynamic scheme for filtering bad-data in sensors networks is developed in [24] where higher filtering capacity is achieved. A pre-estimation based algorithm is developed in [25] to limit

A. S. Musleh and A. Al-Durra are with the department of Electrical and Computer Engineering, Khalifa University of Science and Technology, Sas Al-Nakhl Campus, Abu Dhabi, UAE, Email: amusleh@pi.ac.ae; aaldurra@pi.ac.ae

H. M. Khalid is with the department of Electrical and Electronics Engineering, Sharjah Higher Colleges of Technology (SHCT), University City, Sharjah, UAE, Email: harism.khalid@yahoo.com, Website: www.harismkhalid.com

S. M. Muyeen is with the department of Electrical and Computer Engineering, Curtin University, Perth, WA, Australia, Email: sm.muyeen@curtin.edu.au

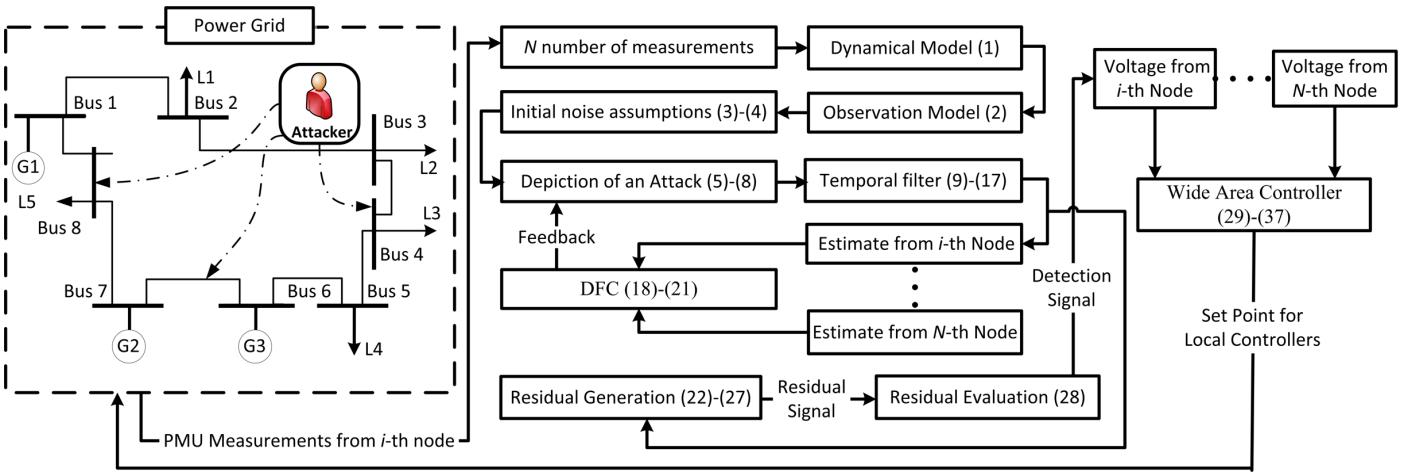

Fig. 1. Proposed TPWAC scheme for WACS application: A reactive power voltage control example

the malicious attacks' effect on power state estimation. Sparsity concept is employed in [26] for detecting bad-data injections in smart grid. Authors of [27] proposed a whole network-aware mitigation algorithm of data employed in state estimation which yields a correct estimation process. Detection of bad data injections in power grid oscillations is deeply investigated in [28,29], where a distributed estimation scheme based Bayesian algorithm and a track fusion-based model prediction are utilized. Distributed filtering architecture provides an enhanced filtering and attacks detection capabilities as suggested in [30]. To the authors' best knowledge, no work has been reported on the mitigation techniques of false data-injection attacks on the phasor measurements, which are collected from the actual PMUs with real-time data flow, and further used for the voltage control in WACMS applications.

Inspired from the above, this work contributes towards developing a real-time based signal processing solution to enhance the resilience of voltage measurements against cyber-attacks as well as cyber-physical attacks and device malfunction. A temporal-prediction based wide-area controller is framed to augment the resilience of the grid against the polluted measurements and tackle the voltage control of the grid adaptively. This will shrink the potential tribulations of bad-data injection attacks. Consequently, a correct set-point of voltage will be sent for the reactive power source realized via the static synchronous compensator (STATCOM) in this study, which is a shunt power electronics based flexible AC transmission system (FACTS) device [31]. This device controls the voltage magnitude by modifying the reactive power generation or absorption.

A brief flowchart of the proposed methodology is shown in Fig. 1. Here, the attacker is able to imitate regular variations of voltage magnitude's data used for voltage control in the power grid. The temporal prediction based filter (TPF) is applied at each i-th node to the magnitude of voltage collected via PMUs. It starts by evolving the system models (1)-(4), where the nonlinear dynamical model (1), observation model (2), and initial noise assumptions (3)-(4) are developed. This is followed by depiction of an attack using observation analysis (5)-(8), which helps to determine the impact of an attack on the collected measurements. This is tackled further using the TPF via modifying the estimated voltage magnitudes at all of the observable nodes (9)-(17). This is achieved via developing a suitable gain and covariance matrices in the presence of an attack. Then, the distributed fusion center (DFC) is framed for the error minimization of filtering and estimation at each PMU (18)-(21). After that, the filter is applied to reveal the injected information by generating the residual (22)-(27). This measure is employed in quantifying the injected information. In evaluating the residual, a threshold is determined (28). Once, the voltage magnitude is collected with the evaluation of fault-injection, the wide-area controller is used to determine the set-point for the local-area controller (29)-(37). The proposed algorithm is tested via a sophisticated real-time experimental setup developed in [32].

The paper is framed as follows: The proposed scheme is detailed in Section II. The implementation and evaluation of a realistic case is discussed in section III, and the concluding remarks are drawn in Section IV.

II. Proposed TPWAC Scheme Formulation

Consider a smart grid susceptible to bad-data injection assault. Each bus in the power grid is observable by a PMU, which is also referred to as a node. It is assumed that all of the PMUs employed operate at the same sampling rate at the instant of time t, and there is no data lack from the PMU nodes. Moreover, the model has the capacity to collect observations as:

$$x_{t+1} = f(x_t, u_t, d_t) + \nu_t^i, t = 0, 1..., T \quad (1)$$

$$z_t^i = H_t^i x_t + w_t^i, i = 0, 1, ..., N \quad (2)$$

where $f(x_t, u_t, d_t)$ is the recognized non-linear function describing the state transition model, r is the state vector dimension in the subspace $\mathbf{R}$, $x_0 \in \mathbf{R}^r$ is the initial state, t is the discrete-time instant, $\nu_t \in \mathbf{R}^r$ is the random load fluctuation based on process noise, and T is the total number of time instants considered. Referring to (2), N is the number of PMU installed at the grid substations, $z_t^i \in \mathbf{R}^{p^i \times r}$ is the vector of observation of the measurements at the i-th node, p^i is the domestic simultaneous observation number made by the i-th node, $H_t^i \in \mathbf{R}^{p^i \times r}$ is the domestic observation matrix at the i-th node, x_t is the state vector for measurements, and $w_t^i \in \mathbf{R}^{p^i}$ is the lo-

cal observation noise. Note that the system noises (w_t and ν_t) are assumed initially uncorrelated with white Gaussian zero-mean. Given that, the proposed scheme can be formulated at every PMU node in a distributed architecture after we construct the observation model using the collected synchrophasor measurements. Computation of individual measurement state x_t is required to find an estimate of a state which is vulnerable to data-injection attacks. However, this is not reasonable since H_t is an unobserved measurement latent variable with a probability of an attack. Therefore, a regularization process is necessary for solving this problem. This is achieved by depicting an attack[1]using the observation analysis of measurements at every i-th node at time instant t.

A. Depiction of an Attack using Observation Analysis

The depiction of the unobservable attacks can be made by the conjugate-prior of distribution of observations. The conjugate-prior is considered here due to its property of using a hyper prior vector which represents the number of observations in each category that is already observed. Let X be the realization of this distribution, f_t^i represents the underlying parameter of an attack or failure given a time sequence T at i-th node, and $z_{pr,t}^i$ represents the predicted synchrophasor observations. The expected value of the underlying attack parameter could be represented as:

$$\mathbf{E}[f_t^i|X, z_t^i] = \frac{z_{pr,t}^i + z_t^i}{T + \sum_{t=1}^{T} z_t^i} \tag{3}$$

This requires the calculation of the maximum *a-posteriori* of the attack parameter f_t^i as:

$$\arg\max_{f_t^i} P(f_t^i|X) = \frac{z_t^i + z_{pr,t}^i - 1}{\sum_{t=1}^{T}(z_t^i + z_{pr,t}^i - 1)} \tag{4}$$

The residual r_{t+1}^i at the time instant for the measured and estimated observation output can be derived as:

$$r_{t+1}^i = z_{t+1}^i - \hat{z}_{t+1|t}^i = z_{t+1}^i - H_t^i(F_t\hat{x}_t^i) \tag{5}$$

Here the bad-data injection attack is characterized by the attack sequence f_t such that:

$$lim\sup \|\Delta x_t\| = \infty, \|\Delta z_t\| \leq 1, t = 0, 1, ..., T \tag{6}$$

where $\|\Delta x_t\| = x_{f,t} - x_t$, $\|\Delta r_t\| = r_{f,t} - r_t$. $x_{f,t}$ and $r_{f,t}$ are the state variables and residual of the compromised system. The temporal prediction-based filter (TPF) can be derived after the attacked PMU nodes have been depicted.

B. Temporal Prediction-based Filter (TPF)

Consider a situation where the attacker is able to hack some of the information from the PMU nodes resulting in loss of information. Specifying such knowledge is practically done by setting the corresponding elements or the eigenvalues of the covariance of x_t to infinity, or setting the corresponding elements or eigenvalues of the inverse of the covariance of state to zero. This is due to the impact of the information loss on the observation matrix and the covariance of the measurement noise.

Consider the observation output in (2) with known $\bar{\nu}_t^i = \mathbf{E}[\nu_t^i]$. A temporal prediction $\hat{x}_{t+1|t}^i$ may exist if and only if a full column rank is noticed for the observation matrix H_t^i, or equivalently $det(H_t^{i^*} H_t^i) \neq 0$. Since there is information loss involved, the resulting state-prediction will have no prior distribution. It will be stated as:

$$\hat{x}_{t+1|t}^i = \mathbf{E}[x_{t+1}^i e_t^{i^*}] R_{e,t}^{i^{-1}} e_t^i = \mathbf{E}[x_{t+1}^i e_t^{i^*}] R_{e,t}^{i^{-1}} (z_t^i - \nu_t^i) \tag{7}$$

where $\nu_t^i \perp z_t^i$, $(\mathbf{E}x_{t+1}e_t^*)R_{e,t}^{-1}$ is derived as the predicted gain matrix indicated via $K_{pr,t}^i$. Due to the information loss of x_t, the computation is likely to give an error due to the affected observation and measurement matrix. This requires computation of H_t and ν_t respectively. Considering information loss of x_t, a positive semi-definite symmetric but singular matrix $H_{x,t}^{-1}$, and cross covariance $H_{xv,t}$, every symmetric matrix could be diagonalized using the orthogonal transformation as follows:

$$H_{x,t}^{-1} = V_t diag(\Lambda_{1,t}, \Lambda_{2,t}) V_t^* \tag{8}$$

where V_t is an orthogonal matrix which diagonalizes $H_{x,t}^{-1}$. Here $\Lambda_{1,t} = diag(\lambda_1, ..., \lambda_n) > 0$, $n_t = rank(H_{x,t}^{-1})$, and $\Lambda_{2,t} = 0$. Now let $[J_{1,t}\ J_{2,t}] = J = V_t^* x_t = [V_{1,t}^*\ V_2^*]x_t$, and $[\bar{J}_{1,t}\ \bar{J}_{2,t}] = \bar{J} = V_t^* \bar{x}_t = [\bar{\nu}_{1,t}\ \bar{\nu}_{2,t}]\bar{x}_t$. Note that $J_{1,t}$ and $\bar{\nu}_{2,t}$ are the sub-vectors of J and $\bar{J}$ that correspond to $\Lambda_{1,t}$, such that $cov(J_1 - \bar{v}_{1,t}) = \Lambda_{1,t}^{-1)}$. Note that $\Lambda_{2,t} = 0$ is equivalent to information loss about $J_{2,t}$. Similarly, the information about x_t contained in $\bar{x}_t$, $H_{x,t}^{-1}$, and $H_{xv,t}$ are equal to that of $J_{1,t}$ included in $\bar{J}$, $\Lambda_{1,t}$, and $cov(J_{1,t}, \nu_t) = V_1^* H_{xv,t}$. Treating $\bar{J}_{1,t}$ as an observation $y_{0,t}$ of $J_{1,t}$ leads to the following data model:

$$y_{0,t} = \bar{J}_{1,t} = J_{1,t} + (\bar{J}_{1,t} - J_{1,t}) = [I, 0]u_t + \nu_{0,t} \tag{9}$$

This results in converting the model in (2) as:

$$y_t = H_t x_t + \nu_t = (H_t)J_t + \nu_t \tag{10}$$

Combining these two models yields:

$$\bar{z}_t = \begin{bmatrix} \bar{J}_{1,t} \\ z_t \end{bmatrix} = \begin{bmatrix} [I, 0] \\ H_t V_t \end{bmatrix} J_t + \begin{bmatrix} \bar{J}_{1,t} - J_{1,t} \\ \nu_t \end{bmatrix} = \bar{H}_t J_t + \bar{\nu}_t \tag{11}$$

The covariance $cov(\bar{v}_t)$ of the measurement noise is calculated via:

$$cov(\bar{\nu}_t) = cov(\begin{bmatrix} \bar{J}_{1,t} - J_{1,t} \\ \nu_t \end{bmatrix}) = \begin{bmatrix} \Lambda_{1,t}^{-1} & -V_{1,t}^* H_{xv,t} \\ -(V_{1,t}^* H_{xv,t})^* & H_t \end{bmatrix} \tag{12}$$

Once $\bar{J}_{1,t}$ is taken as an observation, no prior information about J_t exists at all. Thus, (1) becomes:

$$\hat{x}_{t+1|t}^i = V_t K_t V_t^* \hat{x}_{t+1|t}^i + V_t K_t z_t^i - V_t K_t V_t^* \tag{13}$$

Because at i-th node,

$$\begin{aligned} K_{pr,t}^i &= \mathbf{E}[x_{t+1} e_t^*] R_{e,t}^{i^{-1}} \\ &= H_t^{i^*}[I - P_{t|t-1}^i(1 - H_t^i H_t^{i^*})(P_{t|t-1}^*)(1 - H_t^i H_t^{i^*})^*] \end{aligned} \tag{14}$$

where

$$P_{t|t-1} = cov(x_t^i) - K_t^i cov(z_t^i) K_t^{i^*} = G_t^i Q_t^i G_t^* - K_t R_{e,t}^i K_t^* \tag{15}$$

After deriving the TPF at each i-th PMU node, the process for information fusion takes place.

C. Information Fusion

The information fusion have two steps: 1) Distributed filtering fusion for parameter estimation, and 2) Residual generation.

[1] Since the proposed distributed scheme deem the relationship with the adjacent PMU nodes, the attacks' influence on the adjacent healthful PMU nodes does not influence the gross execution. This is well supported by the fusion center to provide an improved prediction accuracy of the measurements variables with bad-data injections, thus making it not necessary that each substation must be monitored by a PMU. Attacked nodes must be less than the healthy nodes for the algorithm to give reliable results. This case is valid most of the time no entire national grid could be hacked at the one time.

1) Distributed Filtering Fusion: The estimated parameters of every state are fused into the master filter using a distributed architecture outlined in [33], the master filter measurement is stated in the information form as:

$$P^{-1}_{M,t|t}\hat{x}_{M,t|t} = P^{-1}_{M,t|t-1}\hat{x}_{M,t|t-1} + H^{*}_{M,t}R^{-1}_{M,t}z_{M,t} \quad (16)$$

$$P^{-1}_{M,t|t} = P^{-1}_{M,t|t-1} + H^{*}_{M,t}R^{-1}_{M,t}H_{M,t} \quad (17)$$

The variable $P^{-1}_{M,t|t}$ is the new *a-posteriori* estimate covariance matrix of the voltage magnitude. Whereas $P^{-1}_{M,t|t-1}$ is the updated *a-priori* estimate covariance matrix voltage. To integrate the distributed architecture, local observations from N nodes in the network are synthetically implemented into $z_{M,t}\in \mathbf{R}^{pm}$. Similar to (2) the master observation model at t is represented as:

$$z_{M,t} = H_{M,t}x_t + w_{M,t}, \quad (18)$$

They can also be formulated as:

$$z_{M,t}=\begin{bmatrix} z^1_t \\ \vdots \\ z^N_t \end{bmatrix}, H_{M,t} = \begin{bmatrix} H^1_t \\ \vdots \\ H^N_t \end{bmatrix}, w_{M,t} = \begin{bmatrix} w^1_t \\ \vdots \\ w^N_t \end{bmatrix} \quad (19)$$

2) Residual Generation: The generated residual of the estimated parameter relies on two assumptions as follows:

Assumption 1: For every i-th node, L_0 exists so that for every norm bounded $x^i_{1,t}, x^i_{2,t} \in \mathbf{R}^n$, the beneath inequality holds:

$$\|f(u^i_t, z^i_t, x^i_{1,t}) - f(u^i_t, z^i_t, x^i_{2,t})\| \leq L_0\|x^i_{1,t} - x^i_{2,t}\| \quad (20)$$

Assumption 2: Taking into consideration the simplified form of (1), the transfer-function matrix $H^i_t[sI-(A^i_t-K^i_tH^i_t)]^{-1}B^i_t$ is precisely positive real, where $K^i_t \in \mathbf{R}^{n\times r}$ is selected to stabilize $A^i_t - K^i_tH^i_t$.

For a given positive-definite matrix $Q^i_t > 0 \in \mathbf{R}^{n\times n}$ at time instant t, there exists covariance matrices $P^i_t = P^{i^*}_t > 0 \in \mathbf{R}^{n\times n}$ and a scalar covariance error R_t at each i-th node such that:

$$(A^i_t - K^i_tH^i_t)^* P^i_t (A^i_t - K^i_tH^i_t) = -Q^i_t,\ P^i_tB^i_t = H^{i^*}_t R^i_t \quad (21)$$

To detect the fault-injection with residual generation at each i-th node, the following is constructed:

$$\hat{x}^i_t = A\hat{x}^i_t + g(u^i_t, z^i_t) + B^i_t\xi_{f,t}f(u^i_t, z^i_t, \hat{x}^i_t) + K^i_t(z^i_t - \hat{z}^i_t) \quad (22)$$

$$\hat{z}^i_t = H^i_t\hat{x}^i_t,\ r^i_t = W_t(z^i_t - \hat{z}^i_t) \quad (23)$$

where the pair (A_t, H_t) are observable. The non-linear term $g(u^i_t, z^i_t)$ depends on u^i_t and z^i_t, which are directly available. The $f(u^i_t, z^i_t, x^i_t) \in \mathbf{R}^r$ is a non-linear vector function of u^i_t, z^i_t and x^i_t. The $\xi^i_t \in \mathbf{R}$ is an unexpectedly changing parameter once a fault-injection happens. W_t is a variable representing the residual weighting matrix. Because the pair (A_t, H_t) have been presumed to be observable, K^i_t can be selected to ensure $A^i_t - K^i_tH^i_t$ is a stable matrix. It is realized as:

$$e^i_{x,t} = x^i_t - \hat{x}^i_t, \quad e^i_{z,t} = z^i_t - \hat{z}^i_t \quad (24)$$

The equations of error could be given via:

$$e^i_{x,t+1} = (A^i_t - K^i_tH^i_t)e^i_{x,t} + B^i_t[\xi^i_t f(u^i_t, z^i_t, x^i_t) - \xi^i_{f,t}f(u^i_t, z^i_t, \hat{x}^i_t)], \text{ and } e^i_{z,t} = H^i_t e^i_{x,t} \quad (25)$$

The above filter is guaranteed to converge using the following theorem.

Theorem 1: With Assumption 2, the filter is asymptotically convergent when no bad-data injection happens ($\xi^i_t = \xi^i_{f,t}$), i.e. $lim_{t\to\infty} e^i_{z,t} = 0$.

Proof of Theorem 1: This is proved in the Appendix. ■

After the residual is computed, evaluations are necessary for the threshold selection used for identifying a false data-injection.

3) Residual Evaluation: The threshold Γ is computed using the difference between voltage state and its resulting prediction denoted by ε. The possible set of observations are iteratively filtered using subsequent measurements with the objective function Ξ as:

$$\Xi = \sqrt{\sum (z^i_t - z^i_{pr,t})^2},\ \Xi = \begin{Bmatrix} fault\, if\, \varepsilon > \Gamma \\ no\, fault\, if\, \varepsilon \leq \Gamma \end{Bmatrix} \quad (26)$$

Once the information fusion for the parameter estimation, residual generation, and evaluation are completed, the next step is to develop an adaptive controller for the information collected from each i-th node respectively.

D. Wide-Area Control: Secondary Voltage Control Method

Considering the secondary level of the voltage control, the dynamics of the slow behavior of the power grid are deemed. In the control problem of this paper, primary voltage controllers are assumed instantaneous. This is because they have a substantially smaller time step than the wide-area controller. Thus, only steady-state power-flow equations are considered for the wide-area controller. By using the decoupling estimation of the active and the reactive power flow in power grid, a linear model could be approximated which defines the relationship between the reactive power and the voltage magnitude [1]. By rearranging grid nodes into controlled and uncontrolled voltage nodes, the following system can be obtained:

$$\begin{bmatrix} \Delta Q_{c,t} \\ \Delta Q_{u,t} \end{bmatrix} = \begin{bmatrix} B_{cc,t}\ B_{cu,t} \\ B_{uc,t}\ B_{uu,t} \end{bmatrix} \begin{bmatrix} \Delta|V_{c,t}| \\ \Delta|V_{u,t}| \end{bmatrix} \quad (27)$$

where Q is the reactive power, $|V|$ is the voltage magnitude, and B is the susceptance. The subscripts c and u are used to represent the voltage-controlled nodes (with voltage controlling device, e.g. STATCOM) and the voltage-uncontrolled nodes (without voltage controlling device), respectively. Further, the following equations are derived:

$$[\Delta Q_{u,t}]_t = -[B_{uc,t}][\Delta|V_{c,t}|] - [B_{uu,t}][\Delta|V_{u,t}|] \quad (28)$$

$$(\Delta|V_{u,t}|) = -[B_{uu,t}]^{-1}([\Delta Q_{u,t}] + [B_{uc,t}][\Delta|V_{c,t+1}|]) \quad (29)$$

where $[\Delta|V_{u,t}|]$ is the difference between the set-point and measured voltage at the voltage-uncontrolled nodes, $[B_{uu,t}]^{-1}[Q_{u,t}]$ is the reactive power disturbance at the voltage-uncontrolled nodes, and $[B_{uu,t}]^{-1}[B_{uc,t}][\Delta|V_{c,t}|]$ is the controlled voltage at the voltage-controlled nodes. Note that the apparent control objective is to select a control action which minimizes the deviation of the voltage magnitude at the voltage-uncontrolled nodes. This requires an objective function of minimizing the voltage deviations $[\Delta|V_{u,t}|]$ as follows:

$$\min \left| -[B_{uu,t}]^{-1}([\Delta Q_{u,t}] + [B_{uc,t}][\Delta|V_{c,t+1}|]) \right|$$
$$\text{subject to } V^{\min}_{c,t} \leq V_{c,t} \leq V^{\max}_{c,t} \quad (30)$$

This problem is generated from the Multi-Input Multi-Output (MIMO) networked system (power grid). Any variation in voltage setpoint at any voltage-controlled node will have a consequence on all other voltage-uncontrolled node in the grid.

Nevertheless, this consequence contrasts from one node to another depending on the electrical coupling between the nodes acknowledged as the electrical distance [1].

Lemma II.1: Consider the model (1)-(2), with no control input, i.e. $u_t = 0$. If the system is asymptotically stable, and a transfer function has been developed from w_t to the observation output z_t, the following is implied:

- $\|G_t\|_2 \leq \gamma$,
- There exist matrices $P_t \geq 0$ and $Z_t \geq 0$ such that

$$\begin{bmatrix} P_t A_t + A_t^* P_t P_t B_t \; P_t B_t \\ B_t^* P_t \qquad -I \end{bmatrix} \leq 0, \begin{bmatrix} P_t \; H_t^* \\ H_t^* \; Z_t \end{bmatrix} \geq 0, \text{trace}(Z_t) \leq \gamma^2 \quad (31)$$

By minimizing the trace, feedback gains for the adaptive controller can be obtained. The feedback of the control is dependent upon the following assumption.

Assumption 3: The initial transition matrix x_0^i from each i-th node and w_t^i are independent for all time instants t, such that $t \geq 0$. This asserts that P_t^i and $\hat{P}_t^i$ are the same. Hence, both of them can be used to characterize the covariance matrix for the feedback. Considering this assumption, P_t^i satisfies the following Lyapunov differential equation:

$$\hat{Q}_t^i = A_t^i P_t^i + P_t^i A_t^{i^*}, \; t \geq 0, \quad (32)$$

where $P_0^i = \mathbf{E}[x_0^i x_0^{i^*}] - \mathbf{E}[x_0^i]\mathbf{E}[x_0^{i^*}]$

Based on Assumption 1 and 2, the value of $\hat{\xi}_t^i$ for an i-th node is set to $\xi_{f,t}^i$ until a bad-data injection is noticed. It is presumed that after a bad-data injection happens, $\xi_t^i = \text{constant} \neq \xi_{f,t}^i$, $|\xi_{f,t}^i| \leq \xi_0^i$. It is defined:

$$e_{x,t}^i = x_t^i - \hat{x}_t^i, \; e_{z,t}^i = z_t^i - \hat{z}_t^i, \; e_{0,t}^i = \xi_{f,t}^i - \hat{\xi}_{f,t}^i \quad (33)$$

The adaptive control is then obtained as:

$$e_{x,t+1}^i = (A_t^i - K_t^i H_t^i) e_{x,t}^i + B_t^i [\xi_{f,t}^i f(u_t^i, z_t^i, x_t^i) - \hat{\xi}_{f,t}^i f(u_t^i, z_t^i, \hat{x}_t^i)], \; e_{z,t}^i = H_t^i e_{x,t}^i \quad (34)$$

The above adaptive reconfiguration is guaranteed to converge via the following theorem.

Theorem 2: Under the Assumption 1 and 2, the system (34) and the following diagnostic algorithm.

$$\Delta \xi_{f,t}^i = \Gamma f^*(u_t^i, z_t^i, \hat{x}_t^i) R_t^i e_{z,t}^i \quad (35)$$

can recognize $lim_{t \to \infty} e_{x,t}^i = 0$ and a bounded $e_{0,t}^i \in L_0^2$. Moreover, $lim_{t \to \infty} e_{\xi,t}^i = 0$ under a constant excitation, where R_t^i is computed by (21), $\Gamma > 0$ is a weighting scalar.

Proof of Theorem 2: This is proved in the Appendix. ■

III. Implementation and Evaluation

A typical IEEE 14 bus multi-machine system has been chosen in this paper. It includes 2 synchronous generators (G) with IEEE type-1 exciters, 3 synchronous condensers (C), 4 two-winding power transformers, 20 transmission lines with Bergeron model, and 11 dynamic impedance loads as shown in Fig. 2. Grid's modeling details are based on [34]. The primary local controller used here is the FACTS device known as STATCOM which has been designed and connected to bus 13 of the power system [31]. PMUs with accuracy class *P* have been placed optimally in order to have a complete observability of the system (each bus of the grid is observable by at least one PMU). The placement of the PMUs in this paper is based on [35], and the sampling rate of the PMUs is 5 samples/second.

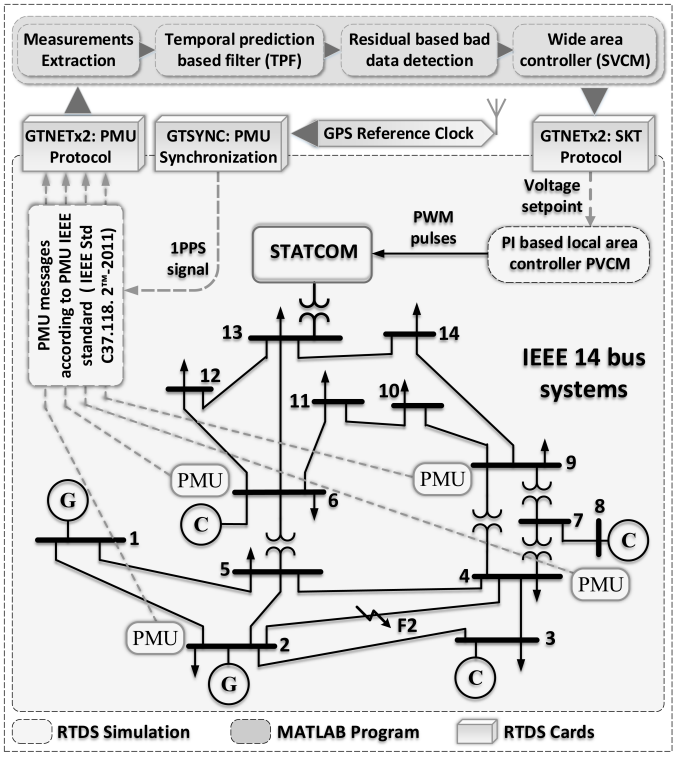

Fig. 2. High-level view of the power grid model, WAMCS with bad-data detection, and the proposed SIL testbed

Real time digital simulator (RTDS) has been used in this study to simulate the power system and the local controller. The PMU model in RTDS is constructed based on the standard IEEE C37.118.1-2011 [12], which makes it reliable. Though, since RTDS is intended purposely for power system models, there is a huge challenge to carry on the big mathematical tasks for the WAMCS in it; consequently, software in the loop (SIL) scheme is adopted. SIL is preferred for advanced validations of embedded control logic in smart grid's studies [36]. A MATLAB built program is employed for the SIL; it starts by creating TCP/IP sockets for the PMUs. Then, it collects the PMU messages according to the IEEE PMU standard C37.118.1-2011 and extracts the measurements. The messages vary in forms and numbers of bytes. For instance, *'AA4100120001448560000F0BBFD00002CE00'* represents a command message for PMU1 to start sending the PMU measurements. The program applies the bad-data detection and wide-area controller equations and sends its action to the local area controller in RTDS. The delay of this program is below 100ms. Two distinctive RTDS cards are used for the SIL: GTSYNC is employed for the synchronization (GPS 1PPS signal) of the PMUs, and GTNETx2 is used for the network communication via two dissimilar protocols (GTNET_SKT for TCP/IP communication, and GTNET_PMU for PMU data transfer according to the IEEE C37.118.1-2011). Figure 2 shows the testing setup for the SIL adopted.

In order to evaluate the proposed methodology, a test case has been designed. This test case has multiple power system disturbances as well as data-injections attacks which are spread over the case duration which is 60 seconds. The power system is distressed by five large disturbances. First, a three-phase-to-

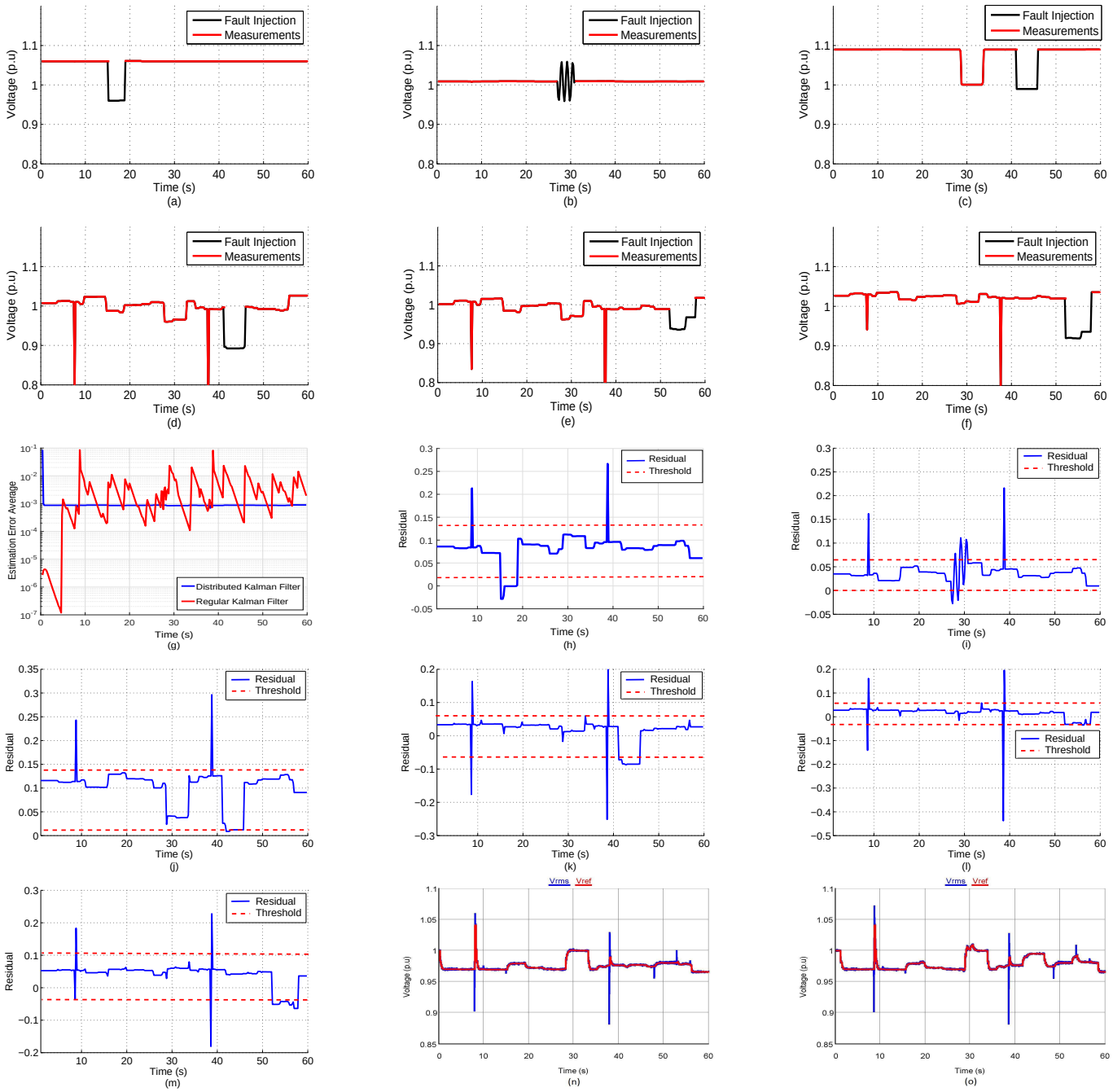

Fig. 3. Profiles of a) Bus 1, b) Bus 3, c) Bus 8, d) Bus 9, e) Bus 10, and f) Bus 11 with random fault injections. Estimation profile of Bus 9 with g) average estimation error. Residual evaluation of h) Bus 1, i) Bus 3, j) Bus 8, k) Bus 9, l) Bus 10, and m) Bus 11 with random fault injections. Wide area controller set-point change n) with and o) without data-injection attacks

ground fault took place at bus 4 at 10 second, and it is cleared within 0.1 seconds. Second, an outage at line 1-5 occurred at 20 second for 5 seconds. Third, a unit outage of a synchronous compensator took place at bus 8 at 30 second for 5 seconds. Fourth, a three-phase-to-ground fault took place at bus 10 at 40 second, and it is cleared after 0.1 seconds. Lastly, an outage at line 2-4 occurred at 50 second for 5 seconds. Furthermore, all of the grid's loads are randomly varied by 10-30 % all of the time, which disturbs the grid's voltage profile.

The proposed method here is evaluated against Kalman filter (KF) technique in [23] which is also a main-stream technique used in the application of power oscillation detection in [37]. However, KF is not originally framed to consider false bad-data injection assaults in WAMCS applications. Similar is the purpose of this paper, where WAMCS is not considered for nominal and healthy conditions. Alternatively, the aim is to have beneficial prudence to the possible variations that may come across via bad-data injection assaults.

To simulate the attacks scenario, several deliberate data-injections have been injected in some of the PMUs measurements. These attacks are equally spread over the case duration and are varied by magnitude and the number of affected measurements. Simulated attack scenarios are as follows:

- *First Injection*: A 0.1 pu voltage decline is injected at bus 1 from 15 to 19 seconds.
- *Second Injection*: Voltage fluctuations at bus 3 are injected

from 27 to 31 seconds.
- *Third Injection*: A 0.1 pu voltage decline is introduced at bus 4, 7, 8, 9 from 41 to 46 seconds.
- *Fourth Injection*: A 0.05 pu voltage decline is introduced at bus 6 and 10 from 52 to 57 seconds, and a 0.1 pu voltage decline is introduced at bus 11 from 52 to 57 seconds.

The first and second injections imitate bad-data injections experienced when a single measurement device is malfunctioned. Also, it imitates the scenario of physical-attacks imposed on a single measurement device. The third and fourth attacks imitate the scenario of the cyber-attacks imposed on more than one measurement device. The third attack represents the aim of bringing down a regional voltage which consists of multiple busses. The fourth attack represents a smart attack where the attacker is trying to imitate a voltage decline at bus 11 which would affect as well the neighboring buses 6 and 10 but with different magnitudes. The aim of injecting a well spread and varied bad-data is to assess the robustness of the proposed scheme. Figures 3 (a-f) show the attacks at some of the affected busses where the black line shows the bad data merged to the clean measurements colored in red.

Figure 3 (g) shows the comparison of estimation error for the proposed scheme with regular Kalman filter. The profile is compared at Bus 9 between 0 to 60 seconds time-window. The proposed scheme demonstrated adequate estimation accuracy. This is due to its property to use a hyper prior vector for the observations having probability of an attack. Furthermore, MSE_x values in Table I show consistent estimation performance of TPF. This is due to the novelty of TPF to recursively construct the loss of information by orthogonal transformation. The magnitude of estimation error is between 10^{-3} and 10^{-4}. This can be further improved if information from more PMU nodes are available to provide a conjugate-prior of the distribution of the observations. In contrast, the estimation accuracy of KF is less. It is due to the linear nature that KF was not able to distinguish the contaminated measurements.

Once the estimation accuracy is guaranteed, the residuals are produced to determine the existence of the data-injection attacks. Fig. 3 (h-m) show the residual generated from the proposed scheme for imposed attacks on buses 1,3,8,9,10 and 11. The figures show the residuals as well as the upper and lower thresholds for each bus. The choice of these thresholds is a very critical procedure as misleading conclusions might be drawn if unappropriated thresholds have been used. In other words, false alarms might be generated for normal measurements generated due to non-attacks grid conditions. It is clear that all the attacks have been detected accordingly. However, the two faults in the case have also crossed the thresholds values in some of the windows. This may give a false alarm for detection of cyber-attacks. This is a normal result as the residual test gives alarms for any unusual measurement variations. This can be further improved by evaluating the harmonics and repeatability of these variations. Furthermore, a comparative study has been made to evaluate the impact of fault-injection attacks on the wide-area controller as shown in Fig. 3 (n-o). It is clear that the main effect of the attack is noticed from 41 to 46 seconds. This is due to the fact that the third attack is a major one where several busses are attacked simultaneously with a voltage decline. This leads the wide-area controller to increase the set-point of the STATCOM as shown in Fig. 3 (o). The effect can also be seen in Table I where MSE_v value is slightly increased due to the impact of injected faults.

TABLE I
MEAN SQUARE ERROR COMPARISONS[1]

Technique	MSE_x	Technique	MSE_v
TPF	1.93×10^{-4}	**WAC_{DI}**	2.93×10^{-2}
KF	1.40×10^{-3}	**WAC_{WDI}**	2.16×10^{-2}

[1]Note that $\text{MSE}_x = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(z_i - x_i)^2}$, $\text{MSE}_v = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(\Delta|V_i|)^2}$, KF, TPF, WAC, DI and WDI, are the state root mean square error, the voltage root mean square error, Kalman filter, Temporal prediction filter, wide area control, data-injection and without data-injection, respectively.

IV. CONCLUSIONS

In conclusion, a novel technique is presented to enhance the resilience of wide-area control systems against the bad-data injections attacks. The temporal prediction attribute of the scheme has assisted to accurately tackle the injection attacks while estimating and controlling the voltage magnitude. In this paper, the developed algorithm has been applied to an advanced wide-area monitoring and control application. Measurements with real-time data flow were taken from the phasor measurement units. The developed scheme was able to elicit the voltage magnitude accurately, which if not detected, may increase the voltage profile deviations, which may lead to voltage instabilities or blackouts. In future, more advanced cases studies shall be considered where adverse and non-regional threats will be tackled.

APPENDIX

1) Proof of Theorem 1:

Consider the following Lyapunov function,

$$V(e_t^i) = e_{x,t}^{i^*} P_t^i e_{x,t}^i \tag{36}$$

where P_t^i is the solution of (21), Q_t^i is chosen such that $\rho_1 = \lambda_{min}(Q_t^i) - 2\|H_t^i\|.|R_t^i|\xi_{f,t}^i L_0 > 0$. Along the trajectory of the fault-free system, the corresponding Lyapunov difference along the trajectory e_t^i is:

$$\begin{aligned}
\Delta V =& \mathbf{E}\{V(e_{t+1}^i|e_t^i, P_t^i)\} - V(e_t^i) \\
=& \mathbf{E}\{e_{t+1}^{i^*} P_t^i e_{t+1}^i\} - e_t^{i^*} P_t^i e_t^i \\
=& (A_{e,t}^i e_{x,t}^i + B_{L_0,t} u_{e,t}^i)^{i^*} P_t^i (A_{e,t}^i e_{x,t}^i + B_{L_0,t}^i u_{e,t}^i) \\
&- e_{x,t}^{i^*} P_t^i e_{x,t}^i \\
=& e_t^{i^*} [(P_t^i (A_t^i - K_t^i H_t^i) + (A_t^i - K_t^i H_t^i)^* P_t^i) \\
&+ P_t^i B_t^i \xi_{f,t}^i [f(u_t^i, z_t^i, x_t^i) - f(u_t^i, z_t^i, \hat{x}_t^i)]] e_t^i
\end{aligned} \tag{37}$$

From Assumption 1 and system described by (21), one can further claim:

$$\begin{aligned}
\Delta V &\leq -e_{x,t}^{i^T} Q_t^i e_{x,t}^i + 2\|e_{z,t}^i\|.|R_t^i|\xi_{f,t}^i L_0 \|e_{x,t}^i\| \\
&\leq -\rho_1 \|e_{x,t}^i\|^2 < 0
\end{aligned} \tag{38}$$

Thus, $\lim_{t\to\infty} e_{x,t}^i = 0$ and $lim_{t\to\infty} e_{z,t}^i = 0$. This completes the proof.

2) Proof of Theorem 2:

Consider the following Lyapunov function,

$$V(e_t^i) = e_{x,t}^{i^*} P_t^i e_{x,t}^i + \Gamma^{-1} e_{\xi,t}^{i^2} \tag{39}$$

From (34) and (35), its first forward difference is:

$$\begin{aligned}\Delta V &= \mathbf{E}\{V(e_{t+1}|e_t^i, P_t^i)\} - V(e_t^i)\\ &= \mathbf{E}\{e_{t+1}^{i^*} P_t^i e_{t+1}^i\} - e_t^{i^*} P_t^i e_t^i\\ &= (A_{e,t}^i e_{x,t}^i + B_{L_0,t}^i u_{e,t}^i)^* P_t^i (A_{e,t}^i e_{x,t}^i + B_{L_0,t}^i u_{e,t}^i)\\ &\quad - e_{x,t}^{i^*} P_t^i e_{x,t}^i\\ &= e_t^{i^*}[(P_t^i(A_t^i - K_t^i H_t^i) + (A_t^i - K_t^i H_t^i)^* P_t^i)\\ &\quad + P_t^i B_t^i [\xi_{f,t}^i f(u_t^i, z_t^i, x_t^i)\\ &\quad - \hat{\xi}_t^i f(u_t^i \xi_t^i, z_t^i, \hat{x}_t^i)] e_t^i - 2 e_{\xi,t}^i f^*(u_t^i, z_t^i, \hat{x}_t^i) R_t^i e_{y,t}^i \end{aligned} \quad (40)$$

According to Assumption 1 and 2, one can state:

$$\begin{aligned}\Delta V \leq & -e_{x,t}^{i^*} Q_t^i e_{x,t}^i - 2 e_{\xi,t}^i f^*(u_t^i, z_t^i, \hat{x}_t^i) R_t^i e_{z,t}^i\\ & 2 e_{x,t}^* H_t^{i^*} R_t^i \{e_{\xi,t}^i f(u_t^i, z_t^i, x_t^i) - \hat{\xi}_t^i f(u_t^i, z_t^i, \hat{x}_t^i)\} \end{aligned} \quad (41)$$

where $\rho_2 = \lambda_{min}(Q_t^i) - 2\|H_t^i\|.|R_t^i|\xi_0^i L_0, |\xi_{f,t}^i| \leq \xi_0^i$, $Q_t^i > 0$ is chosen such that $\rho_2 > 0$. Inequality (41) implies the stability of the origin $e_{x,t}^i = 0$, $e_{\xi,t}^i = 0$, and the uniform boundedness of $e_{x,t}^i$ and $e_{\xi,t}^i$ with $e_{x,t}^i \in L_2$. On the other hand, from (34), $\dot{e}_{x,t}^i$ is uniformly bounded as well. According to Barbalat's Lemma,

$$\lim_{t\to\infty} e_{x,t}^i = 0 \quad (42)$$

The persistent excitation condition means there exist two positive constants σ and t_0 such that for all t the following inequality holds:

$$\sum_{m=t}^{t+t_0} f^*(z_t^i, u_t^i, x_t^i) B_t^{i^*} B_t^i f^*(z_t^i, u_t^i, x_t^i) \geq \sigma I. \quad (43)$$

Subsequently, from (34), (35), (42) and (43), one can conclude that $\lim_{t\to\infty} e_{\xi,t}^i = 0$. This completes the proof.

REFERENCES

[1] J. D. Glover, M. S. Sarma, and T. Overbye, "Power system analysis and design," Stamford: Cengage Learning, 2011.

[2] S. Corsi, "Voltage control and protection in electrical power systems: From system components to wide-area control," London: Springer, 2015.

[3] S. Corsi, M. Pozzi, C. Sabelli and A. Serrani, "The coordinated automatic voltage control of the Italian transmission grid-part I: reasons of the choice and overview of the consolidated hierarchical system," *IEEE Trans. Power Syst.*, vol. 19, no. 4, pp. 1723–1732, 2004.

[4] M. Perron, I. Kamwa, A. Heniche, C. Lafond, P. Cadieux, M. Racine, H. Akremi and S. Lebeau, "Innovative wide-area and local voltage control of dynamic shunt compensation devices to prevent voltage collapse," *CIGRE 2016, Council on Large Electric Systems*, Paris, 2016.

[5] E. Heylen, W. Labeeuw, G. Deconinck and D. V. Hertem, "Framework for evaluating and comparing performance of power system reliability criteria," *IEEE Trans. Power Syst.*, vol. 31, no. 6, pp. 5153–5162, 2016.

[6] Z. Liu and M. D. Ilic, "Toward PMU-based robust automatic voltage control (AVC) and automatic flow control (AFC)," *IEEE General Meeting Power Energy Society*, Minneapolis, 2010.

[7] H. Y. Su and C. W. Liu, "An adaptive PMU-based secondary voltage control scheme," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1514–1522, 2013.

[8] M. Moradzadeh, R. Boel and L. Vandevelde, "Voltage coordination in multi-area power systems via distributed model predictive control," *IEEE Trans. Power Syst.*, vol. 28, no. 1, pp. 513–521, 2013.

[9] R. Bottura and A. Borghetti, "Simulation of the Volt/Var control in distribution feeders by means of a networked multiagent system," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2340–2353, 2014.

[10] J. Ree, V. Centeno and J. Thorp, "Synchronized phasor measurement applications in power systems," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 20–27, 2010.

[11] A. Phadke and J. Thorp, "Synchronized phasor measurements and their applications," *Springer*, 2008.

[12] "IEEE standard for synchrophasor data transfer for power systems," IEEE Std $C37.118.2^{TM}$-2011, *IEEE Power & Energy Society*, New York, 2011.

[13] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," *Proc. IEEE*, vol. 100, pp. 210–224, 2012.

[14] 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.

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

[16] 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.

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

[18] J. Condliffe, "Ukraines Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks," *MIT Technology Review*, Dec. 22, 2016 [Online], Available: https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/.

[19] A. Abur and A. G. Expsito, " Power system state estimation: Theory and implementation," *New York: CRC Press*, 2004.

[20] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "Interleaved hop-by-hop authentication against false data injection attacks in sensor networks," *ACM Trans. Sen. Netwks.*, 2007.

[21] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems J.*, vol. PP, no. 99, pp. 1–9, Jul 2014.

[22] V. Shukla and D. Qiao, "Distinguishing data transience from false injection in sensor networks," *SECON*, 2007.

[23] K. Manandhar, X. Cao, F. Hu, Y. Liu, "Detection of faults and attacks including false data injection attacks in smart grid using Kalman filter," *IEEE Trans. Ctrl. Network Sys.*, vol. 1, no. 4, pp. 370–379, 2014.

[24] Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks," *Proc. IEEE INFOCOM*, 2006.

[25] 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.

[26] 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.

[27] 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.

[28] H. M. Khalid, and J. C.-H. Peng, "A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2026–2037, July 2016.

[29] H. M. Khalid, and J. C.-H. Peng, "Immunity towards data-injection attacks using track fusion-based model prediction," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 697–707, 2017

[30] H. M. Khalid, and J. C.-H. Peng, "Tracking electromechanical oscillations: An enhanced maximum-likelihood based approach," *IEEE Trans. Power Syst.*, vol. 31, no. 3, pp. 1799–1808, 2016.

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

[32] A. S. Musleh, S. M. Muyeen, A. Al-Durra and I. Kamwa, " Testing and validation of wide area control of STATCOM using real time digital simulator with hybrid HIL-SIL configuration," *IET Gen., Transm. Distrib.*, pp. 1-25, 2017.

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

[34] "Power system test case archive," University of Washington: http://www.ee.washington.edu/research/pstca/.

[35] S. Chakrabarti and E. Kyriakides, "Optimal placement of phasor measurement units for power system observability," *IEEE Trans. Pow. Syst.*, vol. 23, no. 3, pp. 1433–1440, 2008.

[36] A. S. Vijay, S. Doolla, M. C. Chandorkar, " Real-time testing approaches for microgrids," *IEEE Jour. of Emer. and Sel. Topics in Pow. Electronics* , pp. 1-22, 2017.

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

Ahmed S. Musleh (S'11) received his B.Sc. (with Highest Honor) from Abu Dhabi University, Abu Dhabi, UAE in 2014, and the M.Sc. from the Petroleum Institute, Abu Dhabi, UAE in 2016, all in Electrical Engineering. He received the Abu Dhabi University Overall Award of Excellence and the Petroleum Institute Graduate Fellowship in 2014 and 2015, respectively. Currently, he is a Research and Teaching Assistant in the Electrical and Computer Engineering Department at Khalifa University of Science & Technology, Sas Al-Nakhl Campus, Abu Dhabi, UAE. His research interests include smart grid technologies, wide-area monitoring and control, power quality issues, and renewable energy integration.

Haris M. Khalid (M'13) received his B.S. (Hons.) degree in Mechatronics and Control Systems Engineering from University of Engineering and Technology (UET), Lahore, Pakistan, in 2007, and the M.S. and Ph.D. degrees in Control Systems Engineering from King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, KSA, in 2009 and 2012, respectively. In 2012, he joined Distributed Control Research Group (DCRG) at KFUPM, as a Research Fellow. From 2013 to 2016, he worked as a Research Fellow with the Power Systems Research Laboratory (PSRL) at iCenter for Energy, Masdar Institute (MI), Masdar City, UAE, which is a MI-MIT Cooperative Program with Massachusetts Institute of Technology (MIT), Cambridge, MA, USA. During this tenure, he was also hired as a Visiting Scholar at Department of Electrical Engineering, Petroleum Institute (PI), UAE. Since 2016, he has been working as an Assistant Professor at Department of Electrical and Electronics Engineering, Higher Colleges of Technology (HCT), UAE. He has authored over 45 peer-reviewed publications, which include one Monograph, seven IEEE Journals, three IET Journals, two Elsevier Journals, three Springer Journals and over 15 peer-reviewed International conferences including the prestigious conferences like American Control Conference, IFAC and IEEE. He has on-going eight years of Research and Development experience, which includes hands-on experience in several research grant-based funded projects including projects with ARAMCO and CAR Research Group. His current research interests include power systems, cyber-physical systems, electric vehicles, signal processing, applied mathematics, fault diagnostics, filtering, estimation, health monitoring, and battery management systems.

S. M. Muyeen (S'03-M'08-SM'12) received his B.Sc. Eng. Degree from Rajshahi University of Engineering and Technology (RUET), Bangladesh formerly known as Rajshahi Institute of Technology, in 2000 and M. Eng. and Ph.D. Degrees from Kitami Institute of Technology, Japan, in 2005 and 2008, respectively, all in Electrical and Electronic Engineering. At the present, he is working as an Associate Professor in the Electrical and Computer Engineering Department at Curtin University, Perth, Australia. He was the recipient of many awards including the Petroleum Institute Research/Scholarship Award 2012. He is the author/co-author of about 200 scientific articles including 70+ journals and 6 Books as Author/Editor. Dr. Muyeen has been given many Keynote and Invited speeches to International Conferences and Universities. His research interests are Renewable Energy, Smart Grid, and Power System Stability. He is serving as Editor/Associate Editor for many prestigious Journals from IEEE, IET, and other publishers, including IEEE Transactions of Sustainable Energy, IEEE Power Engineering Letters, IET Renewable Power Generation, IET Generation, Transmission & Distribution, etc. Dr. Muyeen is the Senior Member of IEEE and Fellow of Engineers Australia (FIEAust).

Ahmed Al-Durra (S'07-M'10-SM'14) received the B.S., M.S., and PhD in Electrical and Computer Engineering from the Ohio State University (OSU) in 2005, 2007, and 2010, respectively. He conducted his PhD research at the Center for Automotive Research in OSU. He joined the Electrical Engineering Department at the Petroleum Institute, Abu Dhabi, UAE as an Assistant Professor in 2010. He obtained the PI Research & Scholarship Award for Junior Faculty in 2014. At the present, he is an Associate Professor in the Electrical & Computer Engineering Department at Khalifa University of Science & Technology, Sas Al-Nakhl Campus, Abu Dhabi, UAE. His research interests are applications of control and estimation theory on power system stability, Micro and Smart Grids, renewable energy, and process control. He has published over 100 scientific articles in Journals, International Conferences, and book chapters. He has successfully accomplished several research projects at international and national levels. He has supervised/co-supervised over 20 PhD/Master students. He is the head of the Energy Systems, Control & Optimization Lab at ADNOC Research & Innovation Center. Dr. Al-Durra is a Senior Member of IEEE.