Detection and Mitigation of False Data Injection Attacks in Networked Control Systems

Arman Sargolzaei, *Member, IEEE*, Kasra Yazdani, Alireza Abbaspour, *Member, IEEE*, Carl D. Crane III, and Warren E. Dixon

***Abstract*—In networked control systems (NCS), agents participating in a network share their data with others to work together. When agents share their data, they can naturally expose the NCS to layers of faults and cyber-attacks, which can contribute to the propagation of error from one agent/area to another within the system. One common type of attack in which adversaries corrupt information within a NCS is called a false data injection (FDI) attack. This article proposes a control scheme, which enables a NCS to detect and mitigate FDI attacks and, at the same time, compensate for measurement noise and process noise. Furthermore, the developed controller is designed to be robust to unknown inputs. The algorithm incorporates a Kalman filter as an observer to estimate agents' states. We also develop a neural network (NN) architecture to detect and respond to any anomalies caused by FDI attacks. The weights of the NN are updated using an extended Kalman filter, which significantly improves the accuracy of FDI detection. A simulation of the results is provided, which illustrates satisfactory performance of the developed method to accurately detect and respond to FDI attacks.**

***Index Terms*—Neural network (NN), extended Kalman filter (EKF), false data injection (FDI) attack, secure control design, security of networked control systems (NCSs).**

NOMENCLATURE

$\alpha_k^{i,l}$	FDI injected to the lth state of the ith agent.
β	Frequency bias factor.
$\hat{\epsilon}$	Estimation of signal ϵ.
λ	EKF gain used in NN.
μ	Damping coefficient.
ω	Speed-droop coefficient.
π	FDI attack function.
Ψ	Feedback control signal.
Σ	Estimation error covariance.
σ	$\tanh$ activation function.
θ	Measurement noise.
Θ	Covariance matrix of process noise.
Ξ	Covariance matrix of measurement noise.
ξ	Process noise.
ζ	Update parameter of the NN.
d	Unknown inputs.
J	Generator moment of inertia.
K_1	Optimal control gain.
K_2	Robust gain for controller.
K_3	Robust gain for observer.
L	Observer filter gain.
M	FDI attacks.
n	Total number of states.
Q, P	State cost and input cost matrices.
$T_{g,i}$	Governor time constant of ith power area.
$T_{tu,i}$	Turbine time constant of ith power area.
U	Control inputs.
W, V	NN learning weights.
X	Aggregate states of the NCS.

I. Introduction

RECENT developments in computing and communications have led to the proliferation of network control systems (NCS) in domains such as distributed power systems and intelligent transportation networks [1]–[3]. In NCS, agents within a network work together to operate, and therefore, it is necessary for them to exchange information. As a network scales, communication between the agents' increases, and due to technological and physical constraints, the data may not be transmitted with proper security protections. Therefore, the interconnection between the agents causes the network to be vulnerable to unforeseen breaches in privacy and security. For example, a distributed power system is heavily reliant on data collected from different entities in the network. In such a system, the security of shared data is key for effective decision making and control. Therefore, it is important to pay meticulous attention to protecting the security of the transmitted data in these networks.

A major concern in NCS security is false data injection (FDI) attacks [4]. An FDI attack is when an adversary gains access to the communication between the components of a NCS and injects data packets that are intentionally inaccurate. NCS are inherently not resilient to unforeseen patterns. A successful FDI attack can cause the state estimation component of a NCS to generate erroneous values, which may lead to unpredictable and

Manuscript received July 20, 2019; revised October 3, 2019; accepted October 14, 2019. Date of publication November 8, 2019; date of current version February 28, 2020. This work was supported by AFOSR under Award FA9550-19-1-0169. Paper no. TII-19-3232. *(Corresponding author: Arman Sargolzaei.)*

A. Sargolzaei, K. Yazdani, C. D. Crane III, and W. E. Dixon are with the Department of Mechanical and Aerospace Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail: a.sargolzaei@gmail.com; kasra.yazdani@ufl.edu; crane@ufl.edu; wdixon@ufl.edu).

A. Abbaspour is with the Department of Advanced Engineering, Hyundai Mobis, Plymouth, MI 48170 USA (e-mail: aabbaspour@mobis-usa.com).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2019.2952067

unstable responses, disrupting a system's operation. In recent years, FDI attacks have been a focus of significant research studies. This article investigates the detection and mitigation of such attacks from a control-theoretic perspective.

In general, FDI attack detection methods in NCSs can be classified into model-based methods [4]–[9] and learning-based methods [10]–[16]. In FDI detection, model-based methods implement an observer to estimate the dynamics of a system. Methods used in this setup include sliding mode observer [5], Kalman filter [4], [6], [9], weighted least square observer [7], and principal component analysis (PCA) [8], [17]. The authors in [5] propose an adaptive sliding mode observer with online parameter estimation for detection and to respond to attacks on agents' states and sensor systems. The work in [9] designs a Kalman filter estimator, a χ^2 detector, and a Euclidean detector for cyber attacks. The authors in [7] design a least-budget defense strategy to protect power systems under FDI attacks. Results such as [8] and [17] incorporate PCA to ensure data integrity in state estimation of power grids. Despite the potential advantages of model-based methods, including real-time anomaly detection and low computational complexity, their high level of dependency on accurate mathematical models makes them vulnerable to model uncertainties and disturbances.

Learning-based FDI detection methods mainly use techniques from artificial intelligence literature for observing a system's states, including neural networks (NN) [10]–[12] and machine learning [13]–[16]. Learning-based methods provide a framework for estimating nonlinear systems that make them a suitable fit for investigating complex dynamical systems. However, such methods impose a significant computational burden on the system, and as a result, they scale poorly. In addition, the stability analysis of learning-based techniques is more complex. Furthermore, the system needs to operate normally during training; otherwise, it will incorporate false data as part of the normal operation of the system, however, this is not always possible in practice.

In this article, an anomaly detection algorithm is developed that leverages model-based observers in combination with learning-based observers to detect and estimate FDI attacks and, at the same time, compensate for uncertainties in the system in real time. The ideas in model-based and learning-based attack detection are combined by incorporating a Kalman filter as an observer and fusing it with a three-layer feed-forward NN observer for detection and estimation of FDI attacks in real time. The proposed algorithm increases the level of security and robustness of the system to model uncertainties, unknown inputs, noisy measurements, and FDI attacks. The learning weights of the NN are updated using an extended Kalman filter (EKF), which improves the performance of the NN along with reducing the response time of the system. Performance of the designed controller is evaluated through numerical simulation and is proven mathematically using the Lyapunov function.

The main contribution of this article rests in designing a resilient and robust framework for controlling NCSs, which can detect and appropriately respond to FDI attacks in realtime. Traditionally, much attention has been focused on the characterization of FDI attacks. However, we focus on investigating the complications of FDI attacks from the perspective of control theory. In short, the contributions of this article are as follows:

1) detection and compensation of FDI attacks in real time;
2) compensating for uncertainties and unknown inputs;
3) Mitigating the computational burden and complexity while increasing the accuracy of learning-based algorithms through incorporating model-based methods;
4) simultaneous detection of FDI attacks on multiple components of a network in the presence of both process and measurement noise;
5) providing stability analysis for the developed control framework.

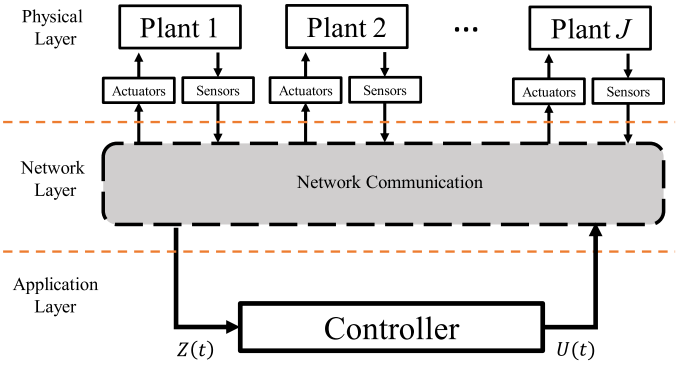

Fig. 1. Illustration of the structure of a CPS in occurrence of FDI attacks on the network.

The rest of this article is organized as follows. The problem formulation is described in Section II. A new algorithm to detect and estimate FDI attacks in a NCS is developed in Section III. In Section IV scheme that is resilient to FDI attacks and robust to uncertainties is developed. In Section V, we formally analyze the performance of our developed controller. An application of a multiagent NCS, namely, a distributed load frequency control (LFC) for a power system is described in Section VI. Finally, Section VII evaluates the performance of the proposed FDI estimation and resilient controller. Section VIII concludes this article.

II. Problem Formulation

A holistic framework of a NCS in form of a cyber-physical system (CPS) is shown in Fig. 1. As illustrated in Fig. 1, a NCS consists of a physical layer, an aggregate network layer, and an application layer where an aggregator collects the data from the network and utilizes the data to make decisions at the network level. The FDI attacks which are the focus of this article take place in the network layer of the NCS, and it is this layer of the network that should be protected against from such attacks.

A. FDI Attacks

An adversary initiates an FDI attack by gaining access to the communication channels among the components of the NCS and by manipulating them. Although FDI attacks have been explored extensively in the literature, it still remains a challenge in NCSs. An adversary's goal is not only to inject incorrect information to disrupt stable operation of the system but also to inject false data such that the system's controller and detection mechanism remain unaware of the issue. Such a hidden attack makes FDI more effective compared with other type of attack [18].

Moreover, a more intelligent adversary may leverage any side-information about the structure of a system in their FDI attacks to make their attacks more destructive. An adversary can perform particular analyses and techniques to gain knowledge about the nominal state values of the agents [19]. A small amount of false data is somewhat detectable and can be filtered using simple filter designs and therefore, an intelligent adversary can inject "reasonable" false data (i.e., close to the nominal states and parameters of the system) into multiple sensors simultaneously. Therefore, FDI is difficult to detect, particularly when the attacker knows the system architecture. In general, an FDI attack can be modeled with a function π which affects the measured feedback signals by

$$\pi(x_k^{i,l}) := x_k^{i,l} + \alpha_k^{i,l} \tag{1}$$

where $\alpha_k^{i,l}$ is the random false data injected to the lth state of the ith agent and $x_k^{i,l}$ denotes the lth state of the ith agent.

B. NCS Under FDI Attack

Consider a NCS consisting of J agents with the following dynamic model

$$\begin{cases} \dot{X}(t) = AX(t) + BU(t) + D\xi(t) + Fd(t) \\ Z(t) = CX(t) + M(t) + \theta(t) \end{cases} \tag{2}$$

where $X(t) \in \mathbb{R}^n$ denotes the aggregate states of the NCS at time t with $n = \sum_{i=1}^{J} n_i$ state variables where n_i is number of states for the ith agent, $U(t)$ is the control input, and $Z(t) = [(z^1(t))^T, (z^2(t))^T, \ldots, (z^J(t))^T]^T$ is the aggregate state measurements of the system. In (2), $M(t) := [(M^1(t))^T, \ldots, (M^J(t))^T]^T, \xi(t)$, and $\theta(t)$ account for the effects of FDI attacks, Gaussian process noise, and measurement noise, respectively, $d(t)$ denotes the unknown inputs, and $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times n}$, $C \in \mathbb{R}^{n\times n}$, $D \in \mathbb{R}^{n\times 1}$, and $F \in \mathbb{R}^{n\times 1}$ are deterministic matrices.

In this article, we introduce the following standard assumptions which help facilitate further development.

Assumption 1: Adversaries do not have access to control signals.

Assumption 2: We assume that $X(0)$ is uncorrelated with the measurement noise and the process noises in the system described in (2), i.e., $\text{cov}[X(0), \xi(t)] = 0$ and $\text{cov}[X(0), \theta(t)] = 0$ for all t. The $\text{cov}[X_0, \xi(t)] = 0$ and $\text{cov}[X_0, \theta(t)] = 0$ for all t, which means that X_0 is uncorrelated with the measurement and the process noises in the system.

Assumption 3: The random variables $\xi(t)$ and $\theta(t)$ are white noise with $\mathbb{E}[\xi(t)] = 0, \mathbb{E}[\theta(t)] = 0$, and $\text{cov}[\xi(t), \theta(t+l)] = 0$ for all t and l.

The covariances of the terms $\xi(t)$ and $\theta(t)$ are defined as

$$\begin{cases} \mathbb{E}[\xi(t)\xi(t+l)^T] := \Xi(t)\delta_{t,l} \\ \mathbb{E}[\theta(t)\theta(t+l)^T] := \Theta(t)\delta_{t,l} \end{cases} \tag{3}$$

where $\Theta(t) \succ 0, \Xi(t) \succeq 0$, and the Kronecker delta function $\delta_{t,l}$ is defined by

$$\delta_{t,l} = \begin{cases} 1 & l = 0 \\ 0 & l \geq 0. \end{cases} \tag{4}$$

Assumption 4: The state's initial values are white noise processes described as $X(0) \sim (\bar{X}, \Sigma(0))$, where $\bar{X}$ denotes the mean and $\Sigma(0)$ is the covariance at initial time.

Remark 1: Stochastic delays on communication channels are small in magnitude and do not have a significant impact on the system stability and, therefore, are disregarded in [20].

III. FDI Detection

In this section, our FFI detection algorithm, consisting of a Kalman filter observer and a NN architecture, is proposed which is able to estimate the states $X(t)$ and outputs $Z(t)$ in real time. The NN weights are updated using an EKF. The EKF is used to increase the accuracy and also response time of the algorithm when the system is under FDI attacks.

A. Observer Design

To completely define the proposed methods, first the architecture of the NN unit is described. In brief, the NN gets the measured system outputs, $Z(t)$, then it updates the weights via a learning algorithm, and finally, it provides the system with appropriate control signals. To reduce the response time of the NN observer, we have incorporated an EKF algorithm, to be described in detail below [21]. The estimates of the agents' states are given by

$$\begin{cases} \dot{\hat{X}}(t) = A\hat{X}(t) + BU(t) + L(Z(t) - \hat{Z}(t)) \\ \hat{Z}(t) = C\hat{X}(t) + \hat{M}(t) \end{cases} \tag{5}$$

where $\hat{X}(t)$ is the state estimate, $\hat{Z}(t)$ is the estimated output, and $\hat{M}(t)$ is the FDI attack estimates. The filter gain L, is given by

$$L(t) = \Sigma(t)C^T\Theta^{-1}. \tag{6}$$

The initial value of the system is assumed to be known and is denoted by $\hat{X}(0) = \mathbb{E}[X(0)]$. The initial value of the covariance matrix Σ is denoted by $\Sigma(0) := \text{cov}(X(0), X(0))$. The rate of change of the covariance matrix of the state estimations, $\dot{\Sigma}(t)$, is given by

$$\dot{\Sigma}(t) = A\Sigma(t) + \Sigma(t)A^T - \Sigma(t)C^T\Theta^{-1}C\Sigma(t) + D\Xi D^T. \tag{7}$$

Furthermore, the update equation for the NN to estimate FDI attacks is given by

$$\hat{M}^i(t) = W^i(t)\sigma\left(V^i(t)\delta^i(t)\right) \tag{8}$$

where $\hat{M}(t) := [\hat{M}^1(t)^T, \ldots, \hat{M}^J(t)^T]^T$. The vectors $W^i(t)$ and $V^i(t) := [V^{i,1}(t), \ldots, V^{i,(a+b)}(t)]$ consist the learning weights of the ith output layer of the NN at time t, $\delta^i(t) := [\hat{M}^i(t-\Delta_t)^T, \ldots, \hat{M}^i(t-a\Delta_t)^T, (e^i(t-\Delta_t)^T, \ldots, (e^i(t-b\Delta_t)^T]^T$, where $a, b \in \mathbb{N}$ are arbitrary positive scalars which are selected according to the required accuracy and computational power. The values a and b determine the size of the NN. The step size of the NN is denoted by Δ_t. We further define the estimation error $e^i(t) := z^i(t) - \hat{z}^i(t)$ and $\sigma(\cdot)$ as an activation function.[1] Now $\hat{M}^i(t)$ can be reformulated as $\hat{M}^i(t) = W^i(t)\sigma(\Gamma^i(t))$, where

$$\Gamma^i(t) = \sum_{\gamma=1}^{a} V^{i,\gamma}(t)\hat{M}^i(t-\gamma\Delta_t) + \sum_{\gamma=1}^{b} V^{i,(a+\gamma)}(t)e^i(t-(a+\gamma)\Delta_t). \tag{9}$$

The FDI attack $\hat{M}(t)$ is recursively updated using the previous a observer inputs and b output errors. To achieve a high level of accuracy and real-time anomaly detection against FDI attacks, the tuning variables a and b are positive values and should be selected based on the application and desired level of accuracy.

B. NN Update Law

The integration of an EKF in updating the weights of the NN is introduced in this section. The EKF improves the convergence rate of the detection and estimation algorithm [22]. The variable k denotes the sampling instance and is defined by $t = k\Delta_t$, where Δ_t is the sampling time. The update parameters for the ith layer of the NN are defined as

$$\zeta_k^i = \left[W_k^i, V_k^{i,1}, \ldots, V_k^{i,a+b}\right]^T. \tag{10}$$

These NN parameters, at each sampling time, are updated according to

$$\zeta_k^i = \zeta_{k-1}^i + \eta^i \lambda_k^i [z_k^i - \hat{z}_k^i] \tag{11}$$

where η_i is the constant learning rate, and λ_k^i is the new Kalman gain for the NN updating unit and is different from the Kalman gain designed for the observer unit. The gain can be calculated as

$$\lambda_k^i = \rho_k^i H_k^i [(H_k^i)^T \rho_k^i H_k^i + \Upsilon_k^i]^{-1} \tag{12}$$

where H_k^i is the derivative of e_k^i with respect to λ_k^i. Based on the observer input in (5), H_k^i can be calculated as

$$H_k^i = \frac{\partial e_k^i}{\partial \lambda_k^i} |_{\zeta_i = \lambda_{k-1}^i} = \begin{cases} \sigma(z_k^i) & \zeta^i = W^i \\ W_k^i \hat{M}_{k-j}^i \acute{\sigma}(z_k^i) & \zeta^i = V^{i,j} \\ W_k^i e_{k-j}^i \acute{\sigma}(z_k^i) & \zeta^i = V^{i,a+j} \end{cases} \tag{13}$$

where ρ_k^i and Υ_k^i are covariance matrices of the state estimation error and noise, respectively, and are computed recursively [23] by

$$\begin{aligned} \rho_k^i &= \rho_{k-1}^i - \lambda_{k-1}^i (H_{k-1}^i)^T \rho_{k-1}^i \\ \Upsilon_k^i &= \Upsilon_{k-1}^i + \frac{(e_k^i)^T(e_k^i) - \Upsilon_{k-1}^i}{k}. \end{aligned} \tag{14}$$

The weights of the NN observer are updated based on (10) and the FDI attacks are estimated using (8). The estimated FDI attack $\hat{M}_k$ is then incorporated in our controller design respond to such attacks in real time.

IV. Controller Design

In NCSs, there is a tradeoff between model accuracy and mathematical complexity. Robust control provides a framework in which system stability under bounded modeling uncertainties is guaranteed. For simplicity, we approximate the nominal dynamics of agents by a linear system and we use robust control to compensate for model uncertainties. Our robust controller synthesis, considers the FDI attack as model uncertainties [24]–[26]. If the attack it is not compensated for, this can naturally lead to degradation of performance and inefficiently. Therefore, a resilient control framework [27] is developed to address the need for attack detection and response. Specifically, we focus on providing a resilient control framework for detection and mitigation of FDI attacks, while we incorporate a robust controller to deal with other uncertainties in the network, which are not caused by attacks. Therefore, we develop a "secure control design" to cover both the robustness and the resiliency aspects [28].

The proposed control system consists of a linear quadratic state-feedback regulator and a feedback controller. Given the dynamical system described in (2), the linear quadratic regulator (LQR) formulation finds the control inputs $U(t)$ which minimize the cost function

$$J = \int_0^\infty \left[X(t)^T Q X(t) + U(t) R U(t)\right] dt \tag{15}$$

for all t, where $Q \succ 0$ and $R \succeq 0$ are known matrices.

We consider an LQR problem in steady state and we assume the pair (A, C) is observable and the pair (A, Ω) is controllable, where $\Xi := \Omega\Omega^T$. Then, the optimal control gain is calculated by $K_1 = R^{-1}B^T P$, where P is a symmetric positive definite matrix, and it is the solution to the following algebraic Riccati equation

$$PA + A^T + Q - PBR^{-1}B^T P = 0. \tag{16}$$

The controller, mitigating the effect of FDI attacks in NCS, is given by

$$U(t) = -K_1\Psi(t) - K_2\Psi(t) \tag{17}$$

where $\Psi(t) := Z(t) - \hat{O}_s(t)$ is the feedback control signal, $\hat{O}_s(t)$ denotes the estimate of the summation of the FDI attack and the measurement noise which is calculated based on (8), $K_2 := \frac{L_s^2}{\varepsilon_2}C^{-1}$, and ε_2 is a small constant of appropriate magnitude [29]. We summarize our control implementation in Algorithm 1.

V. Stability Analysis

Consider the system as described in (2) and we define

$$O_s(t) := M(t) + \theta(t) \tag{18}$$

[1] The results in Section VII use a tanh function, without loss of generality.

Algorithm 1: The Detection Algorithm and the Robust Controller.

```
Data: $A$, $B$, $C$, $D$, $F$, $R$, $Q$, $\Xi$, $\Theta$, $\hat{X}(0)$, and $\Sigma(0)$ are
      known.
begin
    Initialize parameters $0 \leq V(0), W(0) \leq 1$ randomly;
    for $t$ do
        Calculate $\hat{X}$ using (5);
        Calculate $\Sigma(t)$ from (7);
        Update $L(t)$ from (6);
        Compute $\hat{X}(t)$ and $\hat{Z}(t)$ from (5);
        Calculate $\widehat{M}(t)$ from (8);
        Compute $\Gamma^i(t)$ from (9);
        Compute (13) and (14);
        Calculate $\lambda(t)^i$ from (12);
        Update $\zeta(t)^i$ from (11);
        Estimate the FDI attack from (8);
        Calculate $U(t)$ from (17);
```

to account for the FDI attack $M(t)$ and the measurement noise $\theta(t)$. Next, we state the assumptions that are needed to complete our stability analyses.

Assumption 5: The control input is upper-bounded by

$$\|U(t)\| \leq L_u.$$

Assumption 6: The injected FDI attack $O_s(t)$ is upper-bounded by

$$\|O_s(t)\| \leq L_O.$$

Note that Assumption 6 is a standard assumption as adversaries tend to inject attacks in the range of state measurements. Therefore, it is reasonable to assume that the attacks are bounded.

Assumption 7: The norm of the sum of the unknown input and the process noise denoted by $S(t) := Fd(t) + D\xi(t)$ is upper-bounded by

$$\|S(t)\| \leq L_S.$$

Moreover, we present the following lemma which is used later in our stability analyses.

Lemma 1: The symmetric and positive-definite matrix P_L is bounded by

$$\lambda_{\min}(P_L)I_n \leq P_L \leq \lambda_{\max}(P_L)I_n,$$

where $\lambda_{\min}$ and $\lambda_{\max}$ denote the minimum and maximum eigenvalues of the matrix P_L, respectively.

The matrix P_L is the solution to the following Lyapunov equation

$$(A - LC)^T P_L + P_L(A - LC) = -Q_L, \tag{19}$$

where Q_L is a symmetric positive-definite matrix.

Consider the following observer equation

$$\begin{aligned}\dot{\hat{X}}(t) &= A\hat{X}(t) + BU(t) + L(Z - \hat{Z}) + K_3\left(\psi(t) - C\hat{X}(t)\right)\\ \hat{Z} &= C\hat{X}(t) + \hat{O}_s(t),\end{aligned} \tag{20}$$

where $K_3 := \frac{L_s^2}{\varepsilon_3}C^{-1}$, L is the Kalman filter observer gain, and $\psi(t) := Z(t) - \hat{O}_s(t) - C\hat{X}(t)$ is the observer's feedback signal. Subtracting (20) from (2), the estimate of the error system, denoted by $\tilde{x}(t)$, is written as

$$\begin{aligned}\dot{\tilde{X}}(t) &= \dot{X}(t) - \dot{\hat{X}}(t)\\ &= (A - LC)\tilde{X}(t) + S(t) + L\left(O_s(t) - \hat{O}_s(t)\right)\\ &\quad - K_2\left(\psi(t) - \hat{X}(t)\right).\end{aligned} \tag{21}$$

To streamline further analysis, we introduce the following lemma concerning an upper-bound on FDI attack estimates.

Lemma 2: The error in estimation of FDI attack and the measurement noise of the system in (2) can be bounded by

$$\|\left(O_s(t) - \hat{O}_s(t)\right)\| \leq L_a\|\tilde{X}(t)\|, \tag{22}$$

where L_a is finite positive constant.

Proof: See [22]. ■

Theorem 3: The state trajectories of the system defined in (2) under Assumptions (1–7), with the state observer defined by (5–14), and the controller in (17) are globally uniformly ultimately bounded (GUUB) in the sense that

$$\|\Pi(t)\| \leq \sqrt{\frac{\gamma_2}{\gamma_1}\Pi^2(t_0)e^{-\frac{1}{\gamma_2}(t-t_0)} + \gamma_2\varepsilon_1(1 - e^{-\frac{1}{\gamma_2}(t-t_0)})}, \tag{23}$$

where $\Pi := [\tilde{X}^T X^T]^T \in \mathbb{R}^{2n}$, and provided

$$\begin{aligned}&-\lambda_{\min}(Q_L) + 2L_a\lambda_{\max}(P_L(L - K_3))\\ &-\lambda_{\min}(B(K_1 + K_2)) < \varepsilon_4 < 0,\end{aligned} \tag{24}$$

and

$$-\lambda_{\min}(B(K_1 + K_2)) + 2\lambda_{\max}(A - BK_1C) < \varepsilon_5 < 0, \tag{25}$$

where $\lambda(\Omega)$ denotes the eigenvalues of matrix Ω.

Proof: Consider the following continuously differentiable, positive definite, and radially unbounded Lyapunov function candidate

$$V(\tilde{X}, X) = \tilde{X}(t)^T P_L\tilde{X}(t) + X(t)^T X(t), \tag{26}$$

where we have

$$\gamma_1\|\Pi(t)\|^2 \leq V(\tilde{X}, X) \leq \gamma_2\|\Pi(t)\|^2, \tag{27}$$

and where γ_1 and γ_2 are defined as $\gamma_1 := \min(\lambda_{\min}(\{P_L\}, 1)$ and $\gamma_2 := \max(\lambda_{\max}(\{P_L\}, 1)$, respectively. Taking the derivative of (26) and substituting $\dot{\tilde{X}}$ and $\dot{X}$ from (21) and (2), yields

$$\begin{aligned}\dot{V}(\tilde{X}, X) &= \big[A\tilde{X} - LC\tilde{X} + S + L(O_s - \hat{O}_s)\\ &\quad - K_3\left(\Psi - C\hat{X}\right)\big]^T P_L\tilde{X} + \tilde{X}^T P_L\\ &\quad \times \big[A\tilde{X} - LC\tilde{X} + S + L(O_s - \hat{O}_s)\\ &\quad - K_3\left(\Psi - C\hat{X}\right)\big] + X^T\left[AX + BU + S\right]\\ &\quad + \left[AX + BU + S\right]^T X.\end{aligned} \tag{28}$$

Using (17)–(19), (28), can be reformulated to get

$$\begin{aligned}\dot{V}(\tilde{X}, X) &= -\tilde{X}^T Q_L \tilde{X}\\ &\quad + 2\left((O_s - \hat{O}_s)^T (L - K_3)^T\right) P_L \tilde{X} + 2S^T P_L \tilde{X}\\ &\quad - 2\tilde{X}^T (K_3 C)^T P_L \tilde{X} + 2X^T (A - BK_1 C)X\\ &\quad - 2X^T \left(B(K_1 + K_2)(O_s - \hat{O}_s)\right)\\ &\quad + 2X^T S - 2X^T (BK_2 C)X. \end{aligned} \tag{29}$$

Using Lemma 2, we can write

$$\begin{aligned}\dot{V}(\tilde{X}, X) \leq& -\lambda_{\min}(Q_L)\|\tilde{X}\|^2 + 2L_a\lambda_{\max}\\ &\times \left((L - K_3)^T P_L\right) \|\tilde{X}\|^2\\ &+ 2\lambda_{\max}(A - BK_1 C)\|X\|^2\\ &+ 2L_s\|\tilde{X}\| \left(1 - \frac{L_s}{\varepsilon_3}\|\tilde{X}\|\right)\\ &+ 2L_s\|X\| \left(1 - \lambda_{\min}(B\frac{L_s}{\varepsilon_2})\|X\|\right)\\ &- \lambda_{\min}(B(K_1 + K_2))\|\tilde{X}\|^2\\ &- \lambda_{\min}(B(K_1 + K_2))\|X\|^2. \end{aligned} \tag{30}$$

Noting that $2L_s\|\tilde{X}\|(1 - \frac{L_s}{\epsilon}\|\tilde{X}\|) + 2L_s\|X\|(1 - \lambda_{\min}(B\frac{L_s}{\varepsilon_2})$ $\|X\|) \leq \varepsilon_1$, we update (30) to get

$$\begin{aligned}\dot{V}(\tilde{X}, X) \leq& \big[- \lambda_{\min}(Q_L) + 2L_a\lambda_{\max}(P_L(L - K_3))\\ &- \lambda_{\min}(B(K_1 + K_2))\big] \|\tilde{X}(t)\|^2\\ &+ \big[- \lambda_{\min}(B(K_1 + K_2))\\ &+ 2\lambda_{\max}(A - BK_1 C)\big] \|X(t)\|^2\\ &+ \varepsilon_1. \end{aligned} \tag{31}$$

The terms K_1, K_2, and K_3 are design variables and we choose them accordingly to obtain

$$\begin{aligned}\dot{V}(\tilde{X}, X) &\leq -\varepsilon_4\|\tilde{X}(t)\|^2 - \varepsilon_5\|X(t)\|^2 + \varepsilon_1\\ &\leq - \min(\varepsilon_4, \varepsilon_5)(\|\tilde{X}(t)\|^2 + \|X(t)\|^2) + \varepsilon_1\\ &\leq \frac{-1}{\gamma_2} V(\hat{X}, X) + \varepsilon_1. \end{aligned} \tag{32}$$

Based on (27), the differential inequality in (32) can be solved to yield

$$V \leq V_0 \exp\left(-\frac{1}{\gamma_2}(t - t_0)\right) + \gamma_2\varepsilon_1 \left(1 - \exp\left(\frac{-1}{\gamma_2}(t - t_0)\right)\right). \tag{33}$$

■

It should be noted that the proposed control design and anomaly detection technique is general and can be applied to any NCS setup with the dynamic model described as in (2). In the next section, a distributed power system is selected as a particular NCS to investigate the effectiveness of the proposed detection and mitigation framework.

VI. Case Study: LFC for Multiarea Interconnected Power System

Smart grids are modeled as NCSs and they allow for both the utility companies and consumers to monitor and control the power system. The performance of power systems can be disrupted in presence of cyber attacks. FDI attack is a common type of cyber attack that targets data integrity in smart grids [30]–[33]. The dearth of an effective algorithm which is able to alleviate the impacts of FDI attacks can result in system failure [34], which can endanger the providers and consumers [1], [35]. A major cyber attack on interconnected power systems can be as devastating as the Northeast blackout in 2003 [34]. In this article, the effects of FDI attacks on LFC of multiarea interconnected power systems are investigated. The main role of LFC is to maintain short-term load-interchange-generation balance in a smart grid [36]–[38].

A. LFC Model

The mathematical model of LFC system is briefly described here. Consider the dynamic model of the ith power area to be

$$\begin{cases} \dot{x}^i(t) = A_i x^i(t) + B_i u^i(t) + F_i \Delta P_l(t)\\ y^i(t) = C_i x^i(t) \end{cases} \tag{34}$$

where $u^i(t)$ and $\Delta P_l(t)$ are the control input and power deviation due to load variation in the ith power area, respectively. The states of the ith power area are the frequency deviation Δf^i, generator power deviation ΔP_g^i, turbine valve position ΔP_{tu}^i, tie-line power flow ΔP_{pf}^i, and the control error $e^i(t) = \int_0^t (\beta^i \Delta f^i + \Delta P_{pf}^i)dt$, respectively. The deterministic and known matrices A_i, B_i, F_i, and C_i are defined as

$$A_i = \begin{bmatrix} \frac{-\mu_i}{J_i} & \frac{1}{J_i} & 0 & \frac{-1}{J_i} & 0\\ 0 & \frac{-1}{T_{tu,i}} & \frac{1}{T_{tu,i}} & 0 & 0\\ \frac{-1}{\omega_i T_{g,i}} & 0 & \frac{-1}{T_{g,i}} & 0 & 0\\ \sum_{i=j,j=1}^{2} 2\pi T_{i,j} & 0 & 0 & 0 & 0\\ \beta_i & 0 & 0 & 1 & 0 \end{bmatrix} \tag{35}$$

$$B_i = \begin{bmatrix} 0 & 0 & \frac{1}{T_{g,i}} & 0 & 0 \end{bmatrix}^T \tag{36}$$

$$F_i = \begin{bmatrix} \frac{-1}{J_i} & 0 & 0 & 0 & 0 \end{bmatrix}^T \tag{37}$$

where β_i, J_i, ω_i, μ_i, $T_{g,i}$, and $T_{tu,i}$ are the frequency bias factor, generator moment of inertia, speed-droop coefficient, damping coefficient, governor time constant, and turbine time constant for the ith power area, respectively. The parameter $T_{i,j}$ denotes the stiffness constant between the ith and jth power area. The matrix C_i is an identity matrix of appropriate dimension.

B. Multiarea Interconnected LFC Model

The mathematical model of a multiarea interconnected power systems is briefly described in this section. The detailed

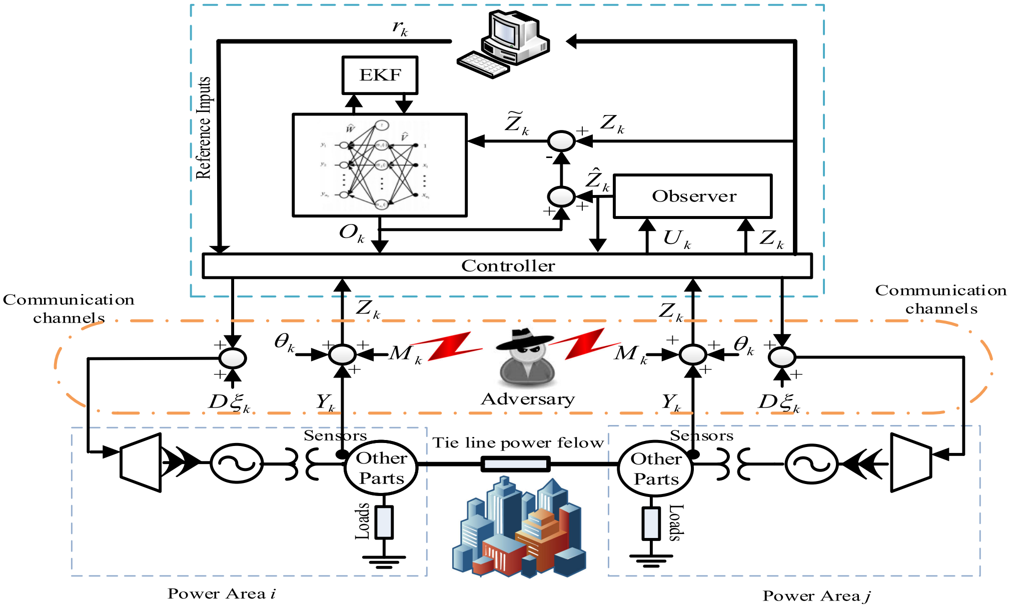

Fig. 2. Schematic diagram of LFC under noise and FDI attacks.

description of the model can be found in [31]. Each power area transmits sensor measurements to a centralized LFC to generate appropriate control signals. Expanding the model described in section A, the dynamic model of a multiarea interconnected power system can be written as

$$\begin{cases} \dot{X}(t) = A_c X(t) + B_c U(t) + F\Delta P_l(t) \\ Y(t) = C_c X(t) \end{cases} \tag{38}$$

where $X(t) = [X_1^T \; X_2^T \; \cdots X_N^T]^T$ are internal states of a N-area interconnected power system and A_c, B_c, C_c, and D_c are known and deterministic matrices defined by

$$A = \begin{bmatrix} A_{1,1} & A_{1,2} & \cdots & A_{1,N} \\ A_{2,1} & A_2 & \cdots & A_{2,N} \\ \vdots & \vdots & \vdots & \vdots \\ A_{N,1} & A_{N,2} & \cdots & A_{N,N} \end{bmatrix} \tag{39}$$

$$B = \text{diag}\left\{ \begin{bmatrix} B_1^T & B_2^T & \cdots & B_N^T \end{bmatrix}^T \right\} \tag{40}$$

where $A_{i,j}$ for $i, j \in \{1, 2, \ldots, N\}$, is given by

$$A_{i,j} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -2\pi T_{i,j} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{41}$$

and C_c is an identity matrix of appropriate dimension.

C. LFC Model Under FDI Attacks

FDI attacks occur when the configuration of a smart grid is exploited to inject false data into certain state measurements. The design of a resilient LFC under FDI attacks requires accurate and real-time information on the location and magnitude of false data injected maliciously to degrade information sharing within components of a network [9], [30]. The article assumes that the authentication credentials can be stolen or the identity of a legitimate component can be used to send unchanged (identity spoofing) or manipulated (content spoofing) messages to other components in a smart grid. Fig. 2 shows a multiarea interconnected power system with automatic gain control under FDI attacks and uncertainties in the communication channels and sensors. Assuming false data can be injected to the communication channels of the system, the model of a multiarea interconnected power system under FDI attacks, measurement noise, and process noise can be defined similar to the system described in (2). In the following section, we consider several scenarios, where FDI attacks are injected to our LFC model and we demonstrate the performance of the proposed estimation algorithm and controller.

VII. Simulation Results and Discussion

The speed and accuracy of the proposed detection algorithm under uncertainties and FDI attacks are evaluated with a two-area interconnected power system with parameters defined in Table I of [31]. For simulation purposes, the discrete-time response of a multiarea power system at sampling intervals $0, \Delta t, 2\Delta t, \cdots$ can be defined as $X(k+1) = e^{A_c\Delta t}X(k) + (\int_0^{\Delta t} e^{A\alpha} d\alpha) B_c U(k)$, where $X(k+1)$ is $X(t)$ at $t = (k+1)\Delta t$ and $\alpha := (k+1)\Delta t - \tau$. The discrete-time model of a multiarea interconnected power system can be

TABLE I
RMSE FOR DETECTING FDI ATTACKS

FDI attack	Traditional AD	Propsoed AD
Scenario I	0.225363	0.068807
Scenario II	0.405883	0.186432
Scenario III*	0.549188	0.133867
Scenario IV	0.232860	0.221108

*Sum of the errors in detection of FDI attacks on the third and eighth states of the LFC system.

defined as

$$\begin{cases} X_{k+1} = A_d X_k + B_d U_k + D\xi_k + F(\Delta P_l)_k \\ Z_k = C_d X_k + M_k + \theta_k \end{cases} \tag{42}$$

where $A_d := e^{A_c \Delta t}$ and $B_d := (\int_0^{\Delta t} e^{A_c \alpha} d\alpha) B_c$.

The power deviation due to load variation in both power areas is simulated using the method discussed in [39]. The simulation time and sampling time are specified to be 10 s and 10 ms, respectively. The designed LQR controller can direct the system toward a stable equilibrium, close to 0 in steady-state error, within a short period of time. Therefore, 10 s of simulation run time is reasonable.

We use root-mean-square error (RMSE) as a measure to evaluate the accuracy of the proposed anomaly detection algorithm in different scenarios for FDI attack, in presence of sensor and measurement noise, for a two-area interconnected power system. The RMSE for this case is defined by

$$\text{RMSE}_i = \sqrt[2]{\frac{\Sigma_{k=1}^{k_f} (\alpha_k^{i,l} - \hat{\alpha}_k^{i,l})^2}{S}} \tag{43}$$

where k_f is the total number of samples time $k\Delta t$.

A. Scenario I: Single Nonperiodic FDI Attack

Consider a scenario in which an FDI attack targets the third state of the first power area, e.g.,

$$\alpha_k^{1,3} = \begin{cases} 0 & 0 < k\Delta_t < 3 \ \& \ k\Delta_t > 8 \\ 0.4 & 3 \leq k\Delta_t \leq 5 \\ 0.9 & 7 \leq k\Delta_t \leq 8 \end{cases}. \tag{44}$$

In Fig. 3, the performance of the proposed anomaly detection algorithm for this case is demonstrated. Our proposed algorithm is able to track the injected FDI step changes more accurately and quicker than a traditional anomaly detection algorithm. The traditional anomaly detection algorithm consists of a Leuenberger observer with a NN-based estimator while the proposed algorithm uses a linear Kalman filter observer and a NN-based EKF attack estimator. Fig. 4 shows the traditional controller is not able to reach the desired value of 0 for both the third and the fifth states, while the proposed resilient controller can compensate for the negative effects of FDI attack.

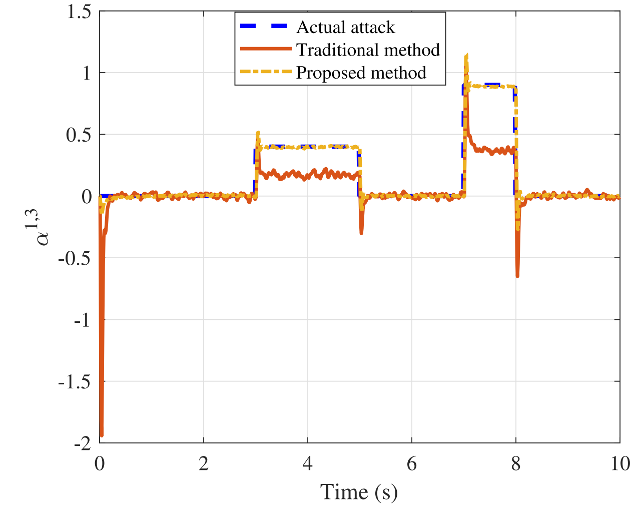

Fig. 3. Scenario I: Estimation of a single nonperiodic FDI attack with the proposed and traditional anomaly detection algorithms.

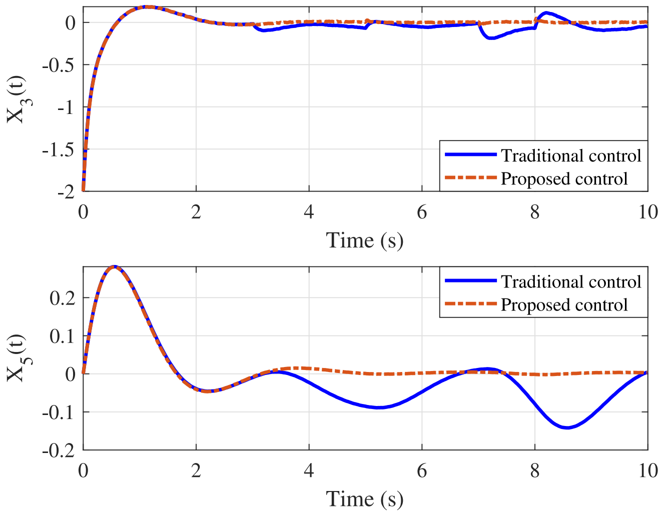

Fig. 4. Scenario I: Performance of the proposed resilient controller and traditional controller in the presence of a single nonperiodic FDI attack.

B. Scenario II: Single Periodic FDI Attack

Consider a case where a single periodic FDI attack is injected into the third state measurement of the first power area as

$$\alpha_k^{1,3} = \begin{cases} 0 & 0 < k\Delta_t < 3 \\ 1.5\sin(10k\Delta_t) & 3 \leq k\Delta_t \end{cases}. \tag{45}$$

Fig. 5 shows the proposed anomaly detection algorithm tracks the magnitude and phase of a single periodic FDI attack accurately. Fig. 6 shows the secure controller performs better than the traditional controller in the presence of a single periodic FDI attack, in the sense that it depicts less oscillations in tracking the states X_3 and X_5. However, the secure controller cannot accurately compensate for the effects of the single periodic FDI attack, since the estimated and actual FDI attacks have a phase lag.

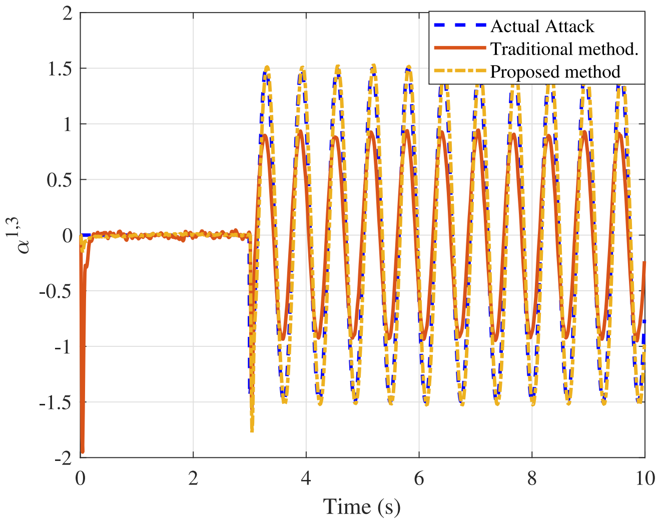

Fig. 5. Scenario II: Estimation of a single periodic FDI attack with the proposed and traditional anomaly detection algorithms.

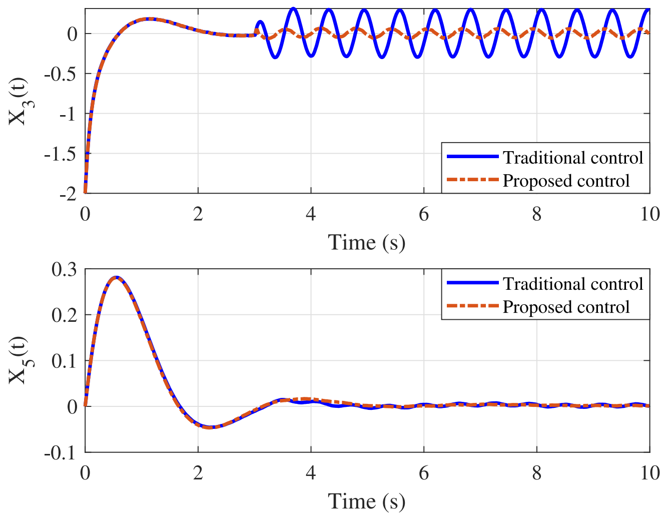

Fig. 7. Scenario II: Performance of the proposed resilient controller and traditional controller in the presence of a single periodic FDI attack with a sampling time of 1 ms.

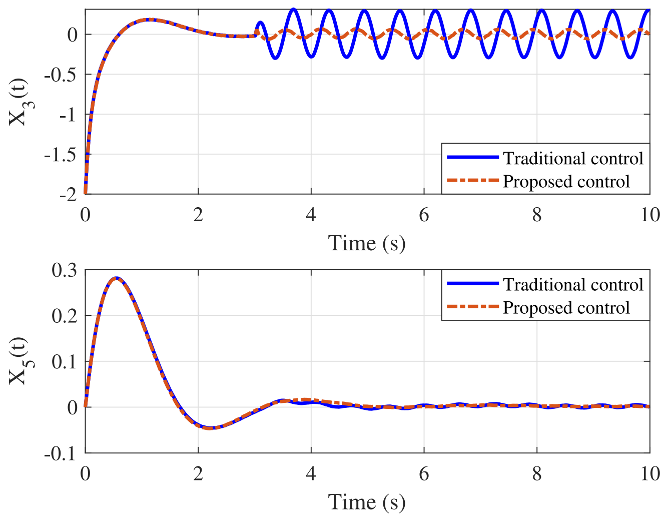

Fig. 6. Scenario II: Performance of the proposed resilient controller and traditional controller in the presence of a single periodic FDI attack with a sampling time of 10 ms attack with the proposed and traditional anomaly detection algorithms.

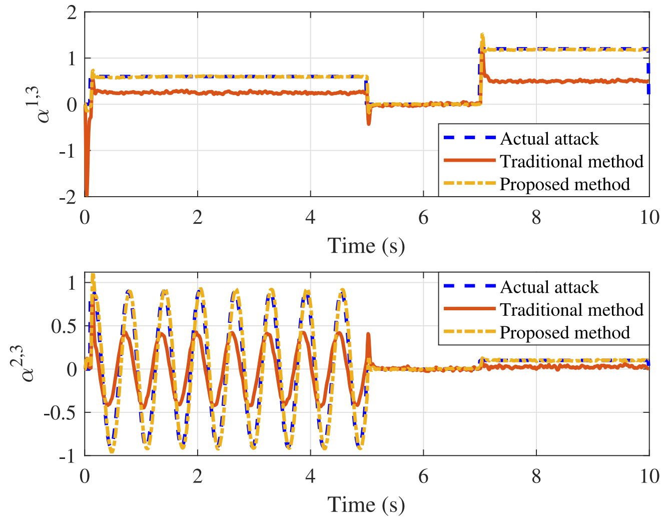

Fig. 8. Scenario III: Estimation of simultaneous FDI attacks with the proposed and traditional anomaly detection algorithms.

This would be improved significantly by increasing the sampling time from 10 to 1 ms, as shown in Fig. 7.

C. Scenario III: Simultaneous FDI Attacks

Consider a scenario in which FDI attacks with different patterns and at different times are injected to multiple state measurements, e.g.,

$$\alpha_k^{1,3} = \begin{cases} 0 & 0 < k\Delta_t < 0.1 \ \& \ k\Delta_t > 8 \\ 0.6 & 0.1 \le k\Delta_t \le 5 \\ 1.2 & 7 \le k\Delta_t \end{cases} \tag{46}$$

and

$$\alpha_k^{2,3} = \begin{cases} 0 & 0 < k\Delta_t < 0.1 \ \& \ k\Delta_t > 8 \\ 0.9\sin(10k\Delta_t) & 0.1 \le k\Delta_t \le 5 \\ 0.1 & 7 \le k\Delta_t \end{cases}. \tag{47}$$

The results for FDI estimation and control compensation are shown in Figs. 8 and 9.

D. Scenario IV: Pulse Train FDI Attack

Fig. 10 compares the estimation of the proposed and traditional anomaly detection algorithms when the FDI attacks have pulse-train asymmetric saw-tooth waveform with saw-tooth width of 0.2 s, repetition frequency of 2 Hz, and skew factor of 1. Fig. 11 illustrates the performance of the proposed secure

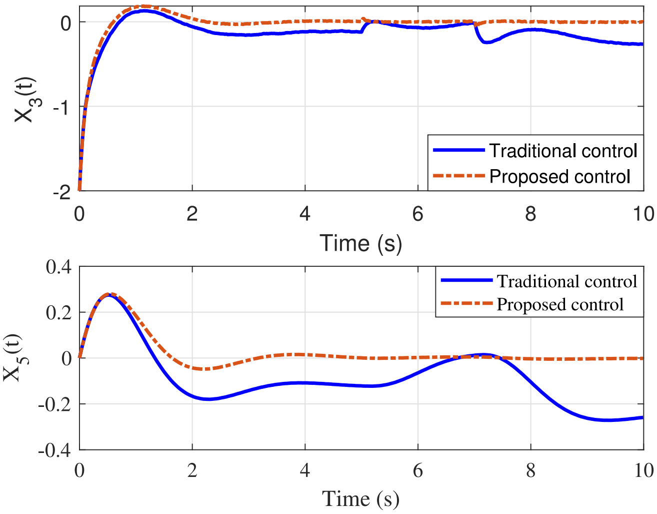

Fig. 9. Scenario III: Performance of the proposed resilient controller and traditional controller in presence of a single periodic FDI attack.

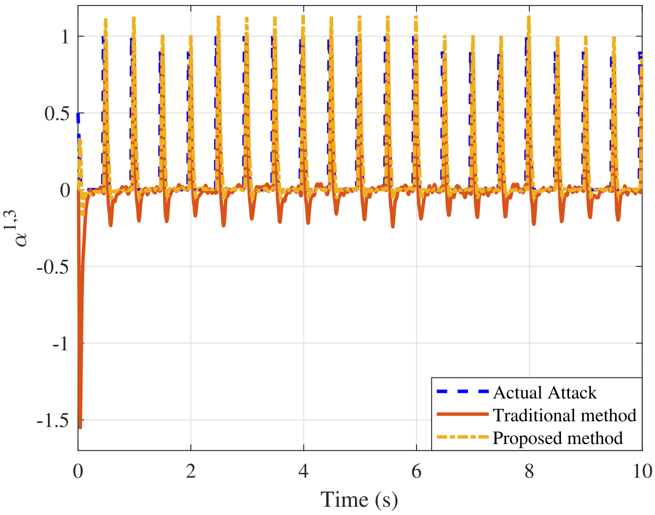

Fig. 10. Scenario IV: Estimation of a pulse-train FDI attack with the proposed and traditional anomaly detection algorithms.

TABLE II
RMSE FOR THE LFC CONTROLLER

FDI attack	Traditional controller	Secure controller
Scenario I	0.066127	0.064231
Scenario II	0.064558	0.064236
Scenario III	0.076106	0.064159
Scenario IV	0.064502	0.064219

*RMSE is calculated for the fifth state of the first power area.

controller and traditional controller in presence of a pulse-train FDI attack. Table I compares the accuracy of the proposed and traditional anomaly detection algorithms, and Table II compares the accuracy of the proposed and the traditional controllers in detecting FDI attacks.

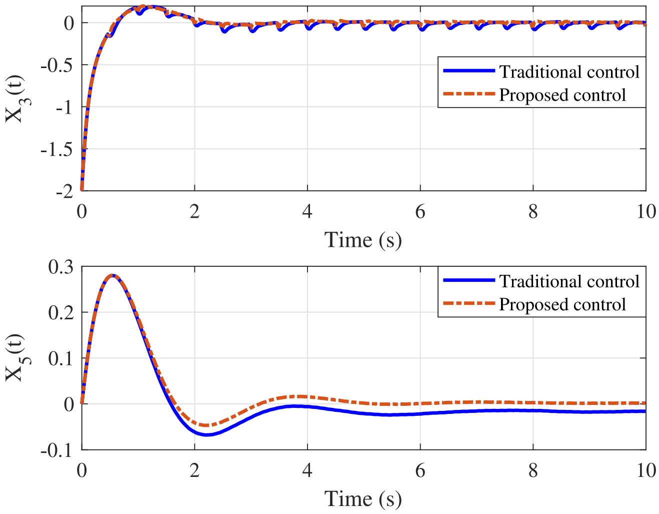

Fig. 11. Scenario IV: Performance of the proposed secure controller and traditional controller in presence of a pulse-train FDI attack.

E. Discussion

Model-based methods are not able to accurately and simultaneously compensate for the effects of uncertainties and FDI attacks, whereas learning-based methods are not able to detect faults in real time for systems with unknown inputs and under process and measurement noises. In our proposed algorithm, significantly lower values of RMSE indicate that adding a NN unit to model-based methods makes them robust to uncertainties. Hence, the developed anomaly detection algorithm can estimate uncertainties and FDI attacks accurately and in a timely manner. Unlike other methods, the developed anomaly detection algorithm is able to detect simultaneous faults and attacks on different states of the system. Furthermore, the developed method eliminates the need for control reconfiguration in presence of FDI attacks, therefore, it reduces costs and complexity.

VIII. Conclusion

This article proposed a secure control strategy for NCSs under measurement noise, process noise, and FDI attacks. Any uncertainty in the system, including FDI attacks, have the potential to make NCSs work inefficiently or become unstable. The developed anomaly detection algorithm consisting of a Kalman filter-based observer and a NN observer can detect and simultaneously compensate for the adverse effects of uncertainties in the system and FDI attacks in real time. The Kalman filter estimated the states of the system. The NN unit provided an estimate of the deviation between the predicted value of the output computed via the linear model and the actual nonlinear system output. In comparison with a traditional fault detection method, the developed anomaly detection algorithm can detect uncertainties and FDI attacks faster and more accurately.

Acknowledgment

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the sponsoring agency.

References

[1] A. Sargolzaei *et al.*, "Detection of and responses to time delays in networked control systems," US Patent 9,946,231, Apr. 17, 2018.

[2] Z. A. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, Dec. 2018.

[3] A. Sargolzaei, "Time-delay switch attack on networked control systems, effects and countermeasures," *FIU Electronic Theses and Dissertations*, 2015, 2175. [Online]. Available: https://digitalcommons.fiu.edu/etd/2175

[4] Z.-H. Pang, G.-P. Liu, D. Zhou, F. Hou, and D. Sun, "Two-channel false data injection attacks against output tracking control of networked systems," *IEEE Trans. Ind. Electron.*, vol. 63, no. 5, pp. 3242–3251, May 2016.

[5] W. Ao, Y. Song, and C. Wen, "Adaptive cyber-physical system attack detection and reconstruction with application to power systems," *IET Control Theory Appl.*, vol. 10, no. 12, pp. 1458–1468, 2016.

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

[7] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 198–207, Feb. 2017.

[8] Z.-H. Yu and W.-L. Chin, "Blind false data injection attack using PCA approximation method in smart grid," *IEEE Trans. Smart Grid*, vol. 6, no. 3, pp. 1219–1226, May 2015.

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

[10] P. Bangalore and L. B. Tjernberg, "An artificial neural network approach for early fault detection of gearbox bearings," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 980–987, Mar. 2015.

[11] A. Abdullah, "Ultrafast transmission line fault detection using a DWT based ANN," *IEEE Trans. Ind. Appl.*, vol. 54, no. 2, pp. 1182–1193, Mar./Apr. 2018.

[12] S. Jana and A. De, "A novel zone division approach for power system fault detection using ann-based pattern recognition technique," *Can. J. Elect. Comput. Eng.*, vol. 40, no. 4, pp. 275–283, 2017.

[13] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016.

[14] J. Yan, H. He, X. Zhong, and Y. Tang, "Q-learning-based vulnerability analysis of smart grid against sequential topology attacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 1, pp. 200–210, Jan. 2017.

[15] S. A. Foroutan and F. R. Salmasi, "Detection of false data injection attacks against state estimation in smart grids based on a mixture gaussian distribution learning method," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 2, no. 4, pp. 161–171, 2017.

[16] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.

[17] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse malicious false data injection attacks and defense mechanisms in smart grids," *IEEE Trans. Ind. Informat.*, vol. 11, no. 5, pp. 1–12, Oct. 2015.

[18] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proc. 1st Int. Conf. High Confidence Netw. Syst.*, 2012, pp. 55–64.

[19] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," in *Proc. IEEE/ACM 3rd Int. Conf. Cyber-Phys. Syst.*, Apr. 2012, pp. 183–192.

[20] A. Sargolzaei, K. K. Yen, and M. Abdelghani, "Time-delay switch attack on load frequency control in smart grid," *Adv. Commun. Technol.*, vol. 5, pp. 55–64, 2013.

[21] I. Rhodes, "A tutorial introduction to estimation and filtering," *IEEE Trans. Autom. Control*, vol. 16, no. 6, pp. 688–706, Dec. 1971.

[22] A. Abbaspour, P. Aboutalebi, K. K. Yen, and A. Sargolzaei, "Neural adaptive observer-based sensor and actuator fault detection in nonlinear systems: Application in UAV," *ISA Trans.*, vol. 67, pp. 317–329, 2017.

[23] L. Ljung and T. Söderström, *Theory and Practice of Recursive Identification*, vol. 5. Princeton, NJ, USA: JSTOR, 1983.

[24] D. C. McFarlane and K. Glover, *Robust Controller Design Using Normalized Coprime Factor Plant Descriptions*, vol. 138. New York, NY, USA: Springer, 1990.

[25] Q. Zhu and T. Başar, "Robust and resilient control design for cyber-physical systems with an application to power systems," in *Proc. 50th IEEE Conf. Decis. Control Eur. Control Conf.*, 2011, pp. 4066–4071.

[26] S. Bhasin, P. Patre, Z. Kan, and W. Dixon, "Control of a robot interacting with an uncertain viscoelastic environment with adjustable force bounds," in *Proc. Amer. Control Conf.*, IEEE, 2010, pp. 5242–5247.

[27] S. Meyn, *Control Techniques for Complex Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2008.

[28] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. IEEE 28th Int. Conf. Distrib. Comput. Syst. Workshops*, 2008, pp. 495–500.

[29] H. K. Khalil, *Nonlinear Control*. London, U.K.: Pearson Higher Ed, 2014.

[30] H. Zhang, W. Meng, J. Qi, X. Wang, and W. X. Zheng, "Distributed load sharing under false data injection attack in inverter-based microgrid," *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1543–1551, Feb. 2019.

[31] A. Sargolzaei, K. K. Yen, and M. N. Abdelghani, "Preventing time-delay switch attack on load frequency control in distributed power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 1176–1185, Mar. 2016.

[32] M. Ghanavati, A. Chakravarthy, and P. P. Menon, "Analysis of automotive cyber-attacks on highways using partial differential equation models," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 4, pp. 1775–1786, Dec. 2018.

[33] A. Abbaspour, A. Sargolzaei, and K. K. Yen, "A neural network based resilient control design for distributed power systems under faults and attacks," in *Proc. IEEE Int. Conf. Environ. Elect. Eng. IEEE Ind. Commercial Power Syst. Eur.*, 2018, pp. 1–6.

[34] J. Hare, X. Shi, S. Gupta, and A. Bazzi, "Fault diagnostics in smart micro-grids: A survey," *Renew. Sustain. Energy Rev.*, vol. 60, pp. 1114–1124, 2016.

[35] A. Sargolzaei, A. Abbaspour, M. A. Al Faruque, A. S. Eddin, and K. Yen, "Security challenges of networked control systems," in *Sustainable Interdependent Networks*. New York, NY, USA: Springer, 2018, pp. 77–95.

[36] C.-K. Zhang, L. Jiang, Q. Wu, Y. He, and M. Wu, "Delay-dependent robust load frequency control for time delay power systems," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2192–2201, Aug. 2013.

[37] M. Ma, C. Zhang, X. Liu, and H. Chen, "Distributed model predictive load frequency control of the multi-area power system after deregulation," *IEEE Trans. Ind. Electron.*, vol. 64, no. 6, pp. 5129–5139, Jun. 2017.

[38] C. Mu, Y. Tang, and H. He, "Improved sliding mode design for load frequency control of power system integrated an adaptive learning strategy," *IEEE Trans. Ind. Electron.*, vol. 64, no. 8, pp. 6742–6751, Aug. 2017.

[39] M. R. Khalghani, J. Solanki, S. Khushalani-Solanki, and A. Sargolzaei, "Stochastic load frequency control of microgrids including wind source based on identification method," in *Proc. IEEE Int. Conf. Environ. Elect. Eng. IEEE Ind. Commercial Power Syst. Eur.*, 2018, pp. 1–6.

Arman Sargolzaei (S'10–M'15) received the M.S. and Ph.D. degrees in electrical and computer engineering from Florida International University (FIU), Miami, FL, USA, in 2012 and 2015, respectively. He is currently working toward the second master's degree in aerospace engineering and the second Ph.D. degree in mechanical engineering from the University of Florida, Gainesville, FL, USA.

He currently holds the position of an Assistant Professor with the Department of Electrical and Computer Engineering, Florida Polytechnic University (FPU), Lakeland, FL, USA. Prior to joining FPU, He was a Faculty Member of Electrical and Computer Engineering with FIU. His mission is to enhance the quality of life for people, with assuring security and privacy concerns through extensive collaboration among multidisciplinary fields.

Dr. Sargolzaei was recognized with the honor of 2017 Faculty Research Excellence and 2018 Faculty Research Excellence award at FPU.

Kasra Yazdani received the B.S. degree in mechanical engineering from Shiraz University, Shiraz, Iran, in 2015, and the M.S. degree in mechanical engineering in 2019 from the University of Florida, Gainesville, FL, USA, where he is currently working toward the Ph.D. degree in mechanical engineering with the Department of Mechanical and Aerospace in Engineering.

His current research interests include privacy and security in multiagent systems, distributed optimization, and machine learning.

Alireza Abbaspour (S'17–M'19) was born in Mashhad, Iran, in 1988. He received the Ph.D. degree in electrical and computer engineering from Florida International University, Miami, FL, USA, in 2018.

He is currently working as a Senior Research Engineer in Autonomous Driving with Hyundai MOBIS Technical Center, Plymouth, MI, USA. He has contributed in several peer-reviewed journals, book chapters, and conferences in the field of his research interests which include nonlinear control systems, fault detection and isolation, fault-tolerant control systems, flight control system.

Carl D. Crane III received the B.S. and M.E. degrees in mechanical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 1978 and 1979, respectively, and the Ph.D. degree in mechanical engineering from the University of Florida, Gainesville, FL, USA, in 1987.

He is currently a Professor with the Department of Mechanical and Aerospace Engineering and Director of the Center for Intelligent Machines and Robotics with the University of Florida. He spent five years as an Officer in the Army Corps of Engineers. He was a Team Leader with the University of Florida's 2004 and 2005 DARPA Grand Challenge autonomous vehicle development efforts and for the University of Florida's 2007 DARPA Urban Challenge project team. He has authored one book and more than 40 papers in the area of spatial geometry and robotic systems. He has supervised 110 master's graduates and 33 Ph.D. graduates during his career at the University of Florida. His research interests include spatial mechanisms, tensegrity systems, robotics, and autonomous navigation for more than 25 years. His current research interests focus on the development and implementation of system architectures for autonomous ground vehicle navigation and the design and implementation of passive parallel mechanisms to be used for force control applications.

Dr. Crane was named a fellow of American Society of Mechanical Engineers (ASME), in 2003.

Warren E. Dixon (M'94–F'16) received the Ph.D. degree from the Department of Electrical and Computer Engineering, Clemson University, Clemson, USA.

He worked as a Research Staff Member and Eugene P. Wigner Fellow at Oak Ridge National Laboratory (ORNL) until 2004, when he joined the University of Florida in the Mechanical and Aerospace Engineering Department. His main research interest has been the development and application of Lyapunov-based control techniques for uncertain nonlinear systems.

Prof. Dixon's work has been recognized by a number of career, society, and best paper awards. He was awarded the Air Force Commander's Public Service Award (2016) for his contributions to the U.S. Air Force Science Advisory Board. He is an American Society of Mechanical Engineers (ASME) Fellow and IEEE Fellow.