Preventing Time-Delay Switch Attack on Load Frequency Control in Distributed Power Systems

Arman Sargolzaei, *Member, IEEE*, Kang K. Yen, *Senior Member, IEEE*, and Mohamed N. Abdelghani, *Member, IEEE*

***Abstract*—A time-delay switch (TDS) attack on a control system is caused by adversaries that strategically imbed time delays into such systems. TDS attacks can make a control system, or more specifically a distributed power control system, unstable. Time delays can be introduced in the sensing loop (SL) or control lines. This paper describes a novel, simple, and effective method to thwart TDS attacks on SL. The proposed method works by augmenting the controller with a time-delay estimator to estimate any time delays. The modified controller controls the system under TDS attack. Also, the time-delay estimator will track time delays introduced by an adversary using a modified model reference control with an indirect supervisor and a modified least mean square minimization technique.**

***Index Terms*—Time-delay switch attack, time-delay estimation, model reference control.**

NOMENCLATURE

Symbol	Definition
$x(t)$	State vector
$\hat{x}(t)$	State estimate vector
$u(t)$	Control vector
ΔP_l	Power deviation of the load
A	Constant matrix
B	Constant matrix
i, j	Power area indices
J	Generator moment of inertia
ω	Speed-droop coefficient
T_{tu}	Turbine time constant
K	The feedback optimal control gain
τ	Time delay in control design
t	Time
ε	Error of the time delay estimation
e_m	Modeling error
$\tau_{\max}$	Maximum time-delay allowed
e	Performance error
Δf	Frequency deviation
Γ	Sampling period
ΔP_g	Power deviation of the generator
ΔP_{tu}	Position value of the turbine
ΔP_{pf}	Tie-line power flow
Λ	Control error
β	Frequency bias factor
μ	Generator damping coefficient
T_g	Governor time constant
T	Stiffness constant
t_d	Time delay in the model
$\hat{\tau}$	Estimate of the time delay
$x(t-\tau)$	Time delayed state
$\hat{x}(t-\hat{\tau})$	Delayed estimate of the state
η	Learning parameter
$r(t)$	Reference signal to be tracked
$\hat{e}$	Estimate of performance error

Manuscript received June 11, 2014; revised January 12, 2015, June 9, 2015, and October 16, 2015; accepted October 31, 2015. Date of publication December 10, 2015; date of current version February 17, 2016. Paper no. TSG-00563-2014.

A. Sargolzaei and K. K. Yen are with the Department of Electrical and Computer Engineering, Florida International University, Miami, FL 33172 USA (e-mail: a.sargolzaei@gmail.com; kang.yen@fiu.edu).

M. N. Abdelghani is with the Department of Mathematics and Statistics, University of Alberta, Edmonton, AB T6G 2G1, Canada (e-mail: mnabdelghani@gmail.com).

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

Digital Object Identifier 10.1109/TSG.2015.2503429

I. INTRODUCTION

TIME DELAYS are ubiquitous in nature. They occur in a wide variety of natural and man-made control systems. Time delays can impact the stability of a system and degrade its performance. A lot of research effort was carried out to understand this issue to control systems with delays [1]–[8].

Time delays exist in power systems, specifically in the sensing and control loops. The traditional controller of power systems is designed based on the availability of current information and ignored time delays. However, power grids are being enhanced by introducing new telecommunication technologies for monitoring to improve the efficiency, reliability and sustainability of supply and distribution. For example, the introduction of a wide-area measurement system (WAMS) provides synchronized, near real-time measurements in phase measurement units (PMUs). WAMS are used for stability analysis of power systems and can be used for efficient controller designs. Nevertheless, time delays are present in PMUs measurements in natural transmission lines [8].

Furthermore, modern power grids rely on computers and multi-purpose networks, which make these type of grids vulnerable to cyber-attacks [1], [3], resulting in major negative impacts on lives and the economy. Investigating the methods of attacks on industrial control systems of sensitive

infrastructures and devising countermeasures and security control protocols have attracted the attention of academia, industries, and governments.

Several studies have considered the problem of stability of power systems with time delays [2]–[8]. The impact of time delays on the power system was discussed in [9]–[13]. In [14] authors studied the effects of including delays on the small signal stability of power systems. In [9] and [10] methods to eliminate oscillations that result from time-delayed feedback control were proposed. Authors in [15] presented a wide-area control system for damping generator oscillations. Using phasor measurements with delays, a controller was proposed in [8], and small signal stability of the power system was considered. A feedback controller designed for power systems with delayed states was proposed in [25]. This controller deals with the combined effects of the instantaneous as well as delayed states using the quadratic Lyapunov function for systems with delays. Additional studies on power systems with delays can be found in [2]–[8] and the references therein. However, most of these studies considered either the construction of controllers that are robust to time delays or controllers that train offline with a time-delay function for estimation. As far as it is known, there are no control methods that perform online estimation of dynamic time delays and real-time control of power systems. Furthermore, few studies [1], [18], [19] considered the control of power systems with time delays introduced by adversary.

This paper will focus on time delays injected by a hacker in a control system, with purpose of destabilizing the system. This kind of attack has been discussed in [18] in the context of power systems (e.g., load frequency control (LFC)) and was named a "time-delay-switch attack" or "TDS" for short in [1], [18], and [19]. To circumvent a TDS attack, system controllers must be redesigned in a way to be robust, or if possible, be able to estimate variable random time delays. This paper will describe a new, easily implementable and effective method to address time-delay switch attacks; that is, a TDS attack on the observed states of a controlled system. The proposed method utilizes a system state estimator, a time-delay estimator, a buffer to store the history of controller commands and a PID or optimal controller to stabilize the plant that tracks a reference signal. For now, only the linear time invariant systems in state feedback will be discussed.

This paper is organized as follows. The next section presents the dynamic of LFC under TDS attack. The control problem and time-delay estimation is formulated in Section III. In Section IV, the detailed simulation results of TDS detection are presented and the time delay and control of a single-input, single-output plant are tracked, as well as the load frequency control for distributed power systems under TDS attack. Finally, some discussion and concluding remarks are presented in Section VI.

II. Model of Power System With TDS Attack

A two-area power plant with automatic gain control under attack is considered in Figure 1. The load frequency controller sends control signals to the plant and obtains state

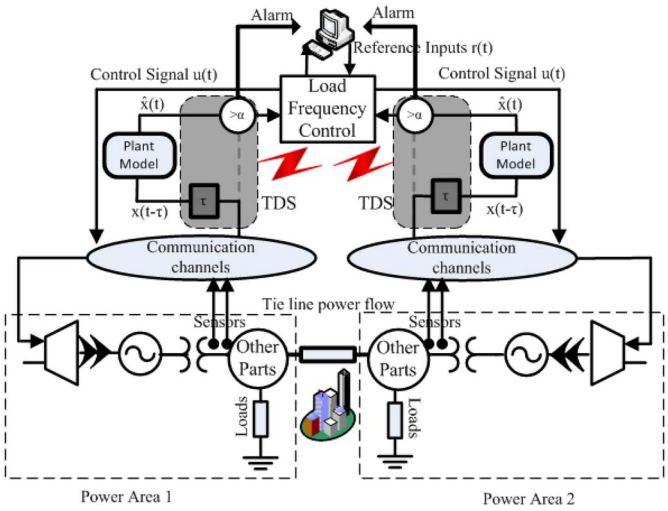


Fig. 1. An adaptive load frequency control for a two-area power system which is robust to the TDS attack using the modified method.

feedback through the communication channels from the turbines and measurements for remote terminal units (RTUs). The communication channels are wireless networks. Attacks can be launched by jamming the communication channels (i.e., DOS attack [16]), by distorting feedback signals (e.g., FDI attack [17]), or by injecting delays (i.e., TDS attack [18], [19]) in data from telemeter measurements.

LFC is usually designed as an optimal feedback controller, but to operate optimally, it requires power state estimations to be telemetered in real time. If an adversary introduces significant time delays in the telemetered control signals or measured states, the LFC will deviate from its optimality and in most cases, the system will break down. In [18], an LFC power system under TDS attack was modeled as a hybrid system, specifically in a switch action, "Off/Delay-by-τ," where τ is some delay time of the sensed system state or the control signals.

The LFC multi-area interlock power system is briefly discussed in [20] and [26]. More details can be found in [27] and [28]. The LFC dynamic model for the i^{th} area is given by

$$\begin{cases} \dot{x}^i(t) = A_{ii}x^i(t) + B_i u^i(t) + h(x^j(t),\ \Delta P_l^i) \\ x^i(0) = x_0^i \end{cases} \tag{1}$$

where $x \in R^5$ and $u \in R^5$ are the state and the control vectors, respectively. The model of the i^{th} area is influenced by the j^{th} power area. Matrices A_{ii} and B_i are constant matrices with suitable dimensions, and ΔP_l^i is the power deviation of the load. The initial state vector is denoted by x_0^i for the i^{th} power area. Then the state vector is defined as

$$x^i(t) = [\ \Delta f^i(t) \quad \Delta P_g^i(t) \quad \Delta P_{tu}^i(t) \quad \Delta P_{pf}^i(t) \quad \Lambda^i(t)\ ]^T \tag{2}$$

where Δf^i, ΔP_g^i, ΔP_{tu}^i, ΔP_{pf}^i and Λ^i are frequency deviation, power deviation of the generator, position value of the turbine, tie-line power flow and control error on the i^{th} power area, respectively [18]. The control error of the i^{th} power area is expressed as

$$\Lambda^i(t) = \int_0^t \beta_i \Delta f^i(s) ds \tag{3}$$

where β_i denotes the frequency bias factor.

In the dynamic model of the LFC, A_{ii}, B_i, and $h(x^j(t),\ \Delta P_l^i)$ are represented by

$$A_{ii} = \begin{bmatrix} -\frac{\mu_i}{J_i} & \frac{1}{J_i} & 0 & -\frac{1}{J_i} & 0 \\ 0 & -\frac{1}{T_{tu\,i}} & \frac{1}{T_{tu\,i}} & 0 & 0 \\ -\frac{1}{\omega_i T_{g\,i}} & 0 & -\frac{1}{T_{g\,i}} & 0 & 0 \\ \sum_{\substack{i\neq j \\ j=1}}^{N} 2\pi T_{ij} & 0 & 0 & 0 & 0 \\ \beta_i & 0 & 0 & 0 & 1 \end{bmatrix} \tag{4}$$

$$B_i = \begin{bmatrix} 0 & 0 & \frac{1}{T_{g\,i}} & 0 & 0 \end{bmatrix}^T \tag{5}$$

$$h(x^j(t),\ \Delta P_l^i) = \sum_{\substack{i\neq j \\ j=1}}^{N} A_{ij}x^j(t) + D_i\Delta P_l^i \tag{6}$$

where N is the total number of power areas, J_i, ω_i, μ_i, $T_{g\,i}$ and $T_{tu\,i}$ are the generator moment of inertia, the speed-droop coefficient, generator damping coefficient, the governor time constant, the turbine time constant in the i^{th} power area, and T_{ij} is the stiffness constant between the i^{th} and the j^{th} power areas, respectively. Also, there is

$$A_{ij} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -2\pi T_{ij} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{7}$$

and

$$D_i = \begin{bmatrix} -\frac{1}{J_i} & 0 & 0 & 0 & 0 \end{bmatrix}^T \tag{8}$$

Equation (9) gives the extension of the dynamic model (1) to the multi-area power system with the attack model using Equations (4), (5), (6), (7) and (8).

$$\begin{cases} \dot{X}(t) = AX(t) + BU(t) + D\Delta P_l \\ X(0) = X_0 \end{cases} \tag{9}$$

where

$$X(t) = \begin{bmatrix} x^1(t)^T & x^2(t)^T & \dots & x^N(t)^T \end{bmatrix}^T \tag{10}$$

$$A = \begin{bmatrix} A_{11} & A_{12} & A_{13} & \cdots & A_{1N} \\ A_{21} & A_{22} & A_{23} & \cdots & A_{2N} \\ A_{31} & A_{32} & A_{33} & \cdots & A_{3N} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{N1} & A_{N2} & A_{N3} & \cdots & A_{NN} \end{bmatrix} \tag{11}$$

$$B = diag\{\begin{bmatrix} B_1^T & B_2^T & B_3^T & \cdots & B_N^T \end{bmatrix}^T\} \tag{12}$$

$$D = diag\{\begin{bmatrix} D_1^T & D_2^T & D_3^T & \cdots & D_N^T \end{bmatrix}^T\} \tag{13}$$

where B and D are $5N\times5N$ matrices.

The optimal feedback controller is given by

$$U = -KX \tag{14}$$

where optimal gain K is $5N\times5N$ matrix, and the control and state signals are 5N×1 matrixes.

The design of the optimal controller for the LFC system in the normal operation (i.e., with no attack) involves minimizing a cost function described by

$$J = \frac{1}{2}\int_0^{t_f} \{X^T(t)\ QX(t) + U^T(t)RU(t)\}dt \tag{15}$$

where the matrix $Q \in \Re^{5N\times5N}$ is positive semi-definite and $R \in \Re^{5N\times5N}$ is positive definite. Then, the optimal control problem is to obtain the optimal control signal $U(t)$ that minimizes the performance index (15), subject to the dynamic of the system with no time delay in its state.

The system with the optimal controller is described by the following equation:

$$\begin{cases} \dot{X}(t) = (A - BK)X(t) + D\Delta P_l \\ X(0) = X_0 \end{cases} \tag{16}$$

With the time-delay attack, the control signal will be modified by

$$U = -K\tilde{X} \tag{17}$$

and the new state after the attack can be modeled by

$$\tilde{X} = \begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \\ \vdots \\ \tilde{x}_N \end{bmatrix} = \begin{bmatrix} x_1(t - t_{d1}) \\ x_2(t - t_{d2}) \\ \vdots \\ x_N(t - t_{dN}) \end{bmatrix} \tag{18}$$

In (18), t_{d1}, t_{d2}, ... and t_{dN} can be different/random time delays and are positive values. When t_{d1}, t_{d2}, ..., t_{dN} are all zero, the system is in its normal operation. An adversary can gain access to the communication link and inject a delay attack on the line to direct the system to abnormal operations.

Remark 1: In this paper, ΔP_l is considered constant. This is a reasonable case, because the stability of power system will not be influenced for an appropriate period following a step load change [20].

In [18] and [19], it was mathematically proved and visually shown that a TDS attack can sabotage and disable the networked control system, and in particular, the LFC system.

To circumvent the detrimental effect of time-delay attacks, control strategies must be developed that are resistant to time delays, and must be able to detect and track the TDS attack and manage a response strategy. A strategy is proposed with the modified method to estimate time-delay attacks from the history of sensed signals. This method can control the system under TDS attack.

III. Methodology

The proposed method involves the use of the plant model, a time-delay estimator, and a PID or optimal controller to control a LTI system with natural delays or a system under TDS attack. The control scheme will detect and track time delays introduced by a hacker and guide the plant to track the reference signal to guarantee the stability for the system.

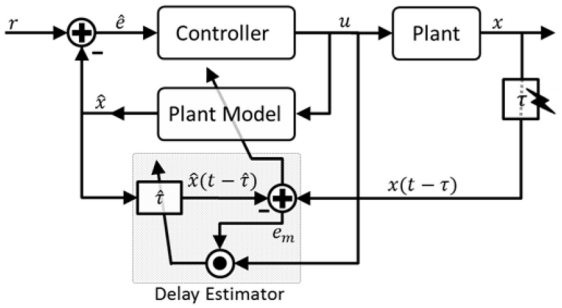


Fig. 2. Block diagram of our proposed control technique.

Figure 2 shows the diagram of the proposed time-delay estimator and controller.

There has been much effort put into the study of time-delayed systems [21]–[23]. For example, Tan [21] proposed two different time-varying time-delay estimation methods using a neural network for a class of nonlinear systems with time-varying time delays. The first method is an indirect time-delay estimator procedure using nonlinear programming. The second is a direct time-delay estimation scheme that uses a neural network to construct a time-delay estimator. The author's method is shown to be more general and accurate than simple linear time-delay estimation procedures [34], [35] for time-varying time-delay signals. However, the methods proposed are complex, and the estimation process takes time to obtain results and work well for periodically reference signals. Chunmao and Jian [22] developed an adaptive control algorithm to guess random time delays in a Networked Control Systems (NCS).

The algorithm updates delay estimation using the gradient descent method, and discovers plant parameters by an improved recursive least square. Authors asserted that the method is superior to the typical networked predictive control. However, the method is complex for even the simplest linear system. Furthermore, the authors did not show results for time-delay control compensation, nor any time tracking of variable delays. Another example of time-delay estimation is the method of variable sampling to compensate for the time delay in a networked control system. A multilayer perceptron (MLP) neural network was used to learn the time delay offline and predict its value during the online control operation [23]. This method assumes that time delay is constant, so it cannot be applied to a system under time-delay attack. All control methods developed in the past to compensate for time delays either rely on a controller that is strong enough to resist a maximum time delay, offline estimates of time delays or approximation of time-delayed signals. This paper proposes a general method for the control of systems under TDS attack. This method was developed for continuous linear time-invariant systems; however, in future work, the result will be extended to a class of nonlinear systems. The models and control strategies to be discussed have been implemented in MATLAB to demonstrate the performance with simulation. Proof of stability will be delegated to another paper and is not in the scope of the current paper.

Suppose the system being dealt with is given by or can be approximated in a region of interest by the LTI system

$$\dot{x}(t) = Ax(t) + Bu(t) \tag{19}$$

and its solution is given by

$$x(t) = e^{At}x_0 + \int_0^t e^{A(t-s)}Bu(s)ds \tag{20}$$

With time delay τ, due to a time-delay switch attack or any natural delay, the solution becomes

$$x(t-\tau) = e^{A(t-\tau)}x_0 + \int_0^{t-\tau} e^{A(t-\tau-s)}Bu(s)ds \tag{21}$$

The solution $x(t)$ at the time t as a function of time-delayed signal $x(t-\tau)$;

$$\begin{aligned} x(t) &= e^{At}x_0 + e^{A\tau}\int_0^{t-\tau} e^{A(t-s)}e^{-A\tau}Bu(s)ds + \int_{t-\tau}^{t} e^{A(t-s)}Bu(s)ds \\ &= e^{At}x_0 + e^{A\tau}\left[x(t-\tau) - e^{A(t-\tau)}x_0\right] + \int_{t-\tau}^{t} e^{A(t-s)}Bu(s)ds \end{aligned} \tag{22}$$

In general, the time delay τ is an unknown variable. The assumption is that τ is a constant value, and $\hat{\tau}$ is the estimate of the time delay τ, then $\varepsilon = \hat{\tau} - \tau$ is the error. The state estimation $\hat{x}(t)$ of the system based on the plant model and the estimate of time delay $\hat{\tau}$ can be calculated as

$$\hat{x}(t) = e^{At}x_0 + e^{A\hat{\tau}}\left[\hat{x}(t-\hat{\tau}) - e^{A(t-\hat{\tau})}x_0\right] + \int_{t-\hat{\tau}}^{t} e^{A(t-s)}Bu(s)ds \tag{23}$$

where $\hat{x}(t-\hat{\tau})$ is the delayed estimate of the state given the estimate of the delay $\hat{\tau}$ (i.e., a simulated signal).

It should be noted that $x(t-\tau)$ is what is actually measured and delivered to the plant model. So, at every instance of time, variables $\hat{x}(t)$, $\hat{x}(t-\hat{\tau})$, $u(t)$, A, B and $x(t-\tau)$ are known to the controller and the plant model. On the other hand, the current state $x(t)$ and the time delay τ are unknown. It is essential that the plant model estimates $x(t)$ correctly. Because of the delay, an accurate estimation of $x(t)$ requires a good estimate of the delay τ. The process will be shown how to estimate delay τ, the state $x(t)$ and control a system using a PID controller and extend the method to an optimal controller.

The modeling error signals in states can be described by $e_m(t) = x(t) - \hat{x}(t)$ and

$$e_m(t;\tau,\hat{\tau}) = x(t-\tau) - \hat{x}(t-\hat{\tau}) \tag{24}$$

The idea is to estimate $\hat{\tau}$ overtime as quickly as possible to minimize the modelling error $e_m(t;\tau,\hat{\tau})$. To do so, let $v = e_m^2/2$. Using the gradient descent method,

$$\frac{d\hat{\tau}}{dt} = -\eta\frac{\partial v}{\partial \hat{\tau}} \tag{25}$$

where η is the learning parameter. The η is set to guarantee convergence of the time-delay estimate to the appropriate time delay as quickly as possible without causing system instability. There many methods for setting the learning parameter η (more details can be found in [33]); however, the choice to use η was based on common sense and knowledge of the system's response.

Following are the calculations of the derivatives of Equation (25):

$$\begin{aligned}\frac{d\hat{\tau}}{dt} &= -\eta\frac{\partial v}{\partial\hat{\tau}}\\ &= -\eta e_m\frac{\partial e_m}{\partial\hat{\tau}}\\ &= -\eta e_m\frac{\partial\big[x(t-\tau)-\hat{x}(t-\hat{\tau})\big]}{\partial\hat{\tau}}\\ &= \eta e_m\frac{\partial\hat{x}(t-\hat{\tau})}{\partial\hat{\tau}}\\ &= \eta e_m\frac{\partial}{\partial\hat{\tau}}\left[e^{A(t-\hat{\tau})}x_0+\int_0^{t-\hat{\tau}}e^{A(t-\hat{\tau}-s)}Bu(s)ds\right]\\ &= \eta e_m\frac{\partial}{\partial\hat{\tau}}\left[\int_0^{t-\hat{\tau}}e^{A(t-\hat{\tau}-s)}Bu(s)ds\right]-\eta e_mAe^{A(t-\hat{\tau})}x_0\\ &= -\eta e_m\Big[Bu(t-\hat{\tau})-e^{A(t-\hat{\tau})}Bu(0)-Ae^{A(t-\hat{\tau})}x_0\Big] \quad (26)\end{aligned}$$

First, let $u(0)=0$, which is reasonable for the initial point, then

$$\frac{d\hat{\tau}}{dt} = -\eta\, e_m\,(Bu(t-\hat{\tau})-Ae^{A(t-\hat{\tau})}x_0), \qquad 0\le\hat{\tau}\le t \quad (27)$$

Equation (27) will be used to estimate the time delay τ. However, there are practical issues that must be considered. Computing machines have finite memory and temporal resolution. Therefore, Equation (27) cannot be implemented without discrete approximation and boundedness assumptions, (see Section IV for details of discrete approximation). To guarantee the stability of calculations and limit memory usage, the following condition must be added; $\tau<\tau_{\max}$. This condition will allow for the construction of a finite buffer that will store the history of $u(t)$ from t to $t-\tau_{\max}$. Also, this will prevent runaway condition on $\hat{\tau}$. It should be noted if the delay injected by an adversary is more than $\tau_{\max}$, a trap condition signal will be sent to the supervisory control and data acquisition (SCADA) center, and the controller will then switch to an open loop control to stabilize the system. This switch is robust since our controller is equipped with a plant model that can predict the next state.

After designing the delay-time estimator, the next step includes the combination of plant model and controller. Let the performance error be $e(t)=r(t)-x(t)$ and the estimate of the performance error be $\hat{e}(t)=r(t)-\hat{x}(t)$. The PID controller is defined input in terms of the estimated error as

$$u(t) = K_P\hat{e}(t)+K_D\frac{d\hat{e}(t)}{dt}+K_I\int_0^t\hat{e}(s)ds \quad (28)$$

and the optimal feedback controller as

$$u(t) = K\hat{e}(t) \quad (29)$$

where K_P, K_D, K_I and K are proportional, derivative, integral and optimal gain, respectively.

The PID controller and optimal feedback controller gains can be designed in normal operation (with no TDS attacks). More details on designing the PID and optimal controllers can be found at [29] and [30], respectively.

The controller has been programmed to depend on the error $\hat{e}(t)$ that results from the estimate $\hat{x}(t)$. If the estimate $\hat{x}(t)$ converges to $x(t)$, then $\hat{e}(t)$ converges to $e(t)$ and is minimized by the controller such that the system $x(t)$ converges to $r(t)$. However, this is not enough; could $\hat{x}(t)$ be estimated when $x(t-\tau)$ is known? This is an important ingredient in finding a stable controller. To answer this question, the following argument must be considered. The plant model estimation equation is given by

$$\dot{\hat{x}}(t) = A\hat{x}(t)+Bu(t) \quad (30)$$

The delayed equation of the state is

$$\dot{x}(t-\tau) = Ax(t-\tau)+Bu(t-\tau) \quad (31)$$

where $x(t-\tau)$ and $\dot{x}(t-\tau)$ are measured by the plant model, and $u(t-\tau)$ is unknown since τ is not known.

Now, the following equation can be considered:

$$\dot{\hat{x}}(t-\tau) = A\hat{x}(t-\tau)+Bu(t-\tau) \quad (32)$$

Elements of Equation (32) are unknown because τ is unknown.

Equation (32) is multiplied by a constant gain matrix $C>0$ and the resultant is subtracted $C\dot{\hat{x}}(t-\tau)$ from $\dot{\hat{x}}(t)$ of Equation (30). In this way, the following is obtained:

$$\begin{aligned}\dot{\hat{x}}(t) = A\hat{x}(t)+C\dot{\hat{x}}(t-\tau)-CA\hat{x}(t-\tau)\\ -CBu(t-\tau)+Bu(t) \quad (33)\end{aligned}$$

Substituting $CBu(t-\tau) = C\dot{x}(t-\tau)-CAx(t-\tau)$ in Equation (33) results in

$$\begin{aligned}\dot{\hat{x}}(t) &= A\hat{x}(t)+Bu(t)+C\dot{\hat{x}}(t-\tau)-CA\hat{x}(t-\tau)\\ &\quad -C\dot{x}(t-\tau)+CAx(t-\tau)\\ &= A\hat{x}(t)+Bu(t)\\ &\quad -C\Big[\dot{x}(t-\tau)-\dot{\hat{x}}(t-\tau)\Big]+CA\big[x(t-\tau)-\hat{x}(t-\tau)\big]\\ &= A\hat{x}(t)+Bu(t)-C[\dot{e}_m(t;\,\tau,\,\tau)-Ae_m(t;\,\tau,\,\tau)]\end{aligned} \quad (34)$$

Note that, the first τ is the actual delay signal that is associated with the delayed signal $x(t\text{-}\tau)$ itself which is read via the communication channel. This τ is hidden and is not accessible to the control system. While the second τ is associated with the plant estimator and estimate of the delay signal $\hat{\tau}$ and delayed states $\hat{x}$, Equation (34) is stated assuming the fact that $\hat{\tau}=\tau$. Now, we replace $e_m(t;\,\tau,\,\tau)$ by $e_m(t;\,\tau,\,\hat{\tau})$ of Equation (24), and obtain

$$\dot{\hat{x}}(t) = A\hat{x}(t)+Bu(t)-C\big[\dot{e}_m(t;\,\tau,\,\hat{\tau})-Ae_m(t;\,\tau,\,\hat{\tau})\big] \quad (35)$$

The above replacement makes the current predicted estimate of the plant state $\hat{x}(t)$ dependent on the estimate of the time delay $\hat{\tau}$. In other words, an accurate estimate of the state depends on an accurate estimate of the time delay.

In Equation (35), only if $\dot{e}_m(t;\,\tau,\,\hat{\tau})-Ae_m(t;\,\tau,\,\hat{\tau})$ equals zero *as a result of* $\hat{\tau}$ converging to τ, then $\hat{x}(t)$ will converge to $x(t)$. This means that the modeling error e_m should be exponentially damped, i.e., $\dot{e}_m(t;\,\tau,\,\hat{\tau})=Ae_m(t;\,\tau,\,\hat{\tau})$.

Notice that the method by which the plant estimate is constructed depends on the measured states of the plant, $x(t-\tau)$, and the estimate of the state given the estimated time delay, $\hat{x}(t-\hat{\tau})$. The difference $x(t-\tau)-\hat{x}(t-\hat{\tau})$ is the modelling error signal $e_m(t;\,\tau,\,\hat{\tau})$.

The choice of the gain matrix C in Equation (35) is dictated by balancing the requirements for having the plant model state depend on errors in time-delays estimation and guarantees that the control system remains stable. More details can be found in [31] and [32].

This method has been implemented in MATLAB, and its performance has been verified using a single input, single output system and an LFC control of two-area distributed power systems. The next section presents and discusses the simulation results.

IV. Algorithm of Controller Design

Step 1: Initialize time-delay estimate $\hat{\tau}$, plant model state estimate $\hat{x}$ and model error e_m. Then, set the learning parameter η to a suitable value. Also, set the matrix C.

Step 2: Obtain a plant state measurement (i.e., the sensed states of the plant $x(t-\tau)$), which could be time-delayed by $\tau(t)$

Step 3: Compute the current state estimate, $\hat{x}(t)$, using Equation (35). In the discrete form Equation (35) can be approximated as:

$$\hat{x}(k+1) = \hat{x}(k) + A\Gamma\hat{x}(k) + B\Gamma u(k) - C[e_m(k) - e_m(k-1) - A\Gamma e_m(k)]$$

where Γ is the sampling period.

Step 4: Compute the delayed plant state estimate $\hat{x}(t-\hat{\tau})$ based on the model equation and the estimate of the performance error $\hat{e}(t) = r(t) - \hat{x}(t)$ and model error $e_m(t;\tau,\hat{\tau}) = x(t-\tau) - \hat{x}(t-\hat{\tau})$

Step 5: Compute the time-delay estimate $\hat{\tau}$, from Equation (27). The discrete approximation of Equation (27) is described below:

$$\hat{\tau}(k+1) = \hat{\tau}(k) - \eta\Gamma e_m(k)\big(Bu(k-\omega) - Ae^{A\Gamma(k-\omega)}x(0)\big),$$

where Γ is the sampling period and $\omega = round\big(\hat{\tau}(k)/\Gamma\big)$ is the nearest integer to $\hat{\tau}(k)/\Gamma$.

Step 6: Compute the control signal $u(t)$. For example, u can be set by using Equation (28 or 29).

Step 7: To prevent runaway conditions, bound the control signal by $\pm u_{max}$, time-delay estimate by $\tau_{\max}$ and plant model by $\pm x_{max}$

Step 8: Repeat steps 2-7 until the estimate of the performance error $\hat{e} < \varepsilon$. In the case of time-delay tracking and tracking of a reference trajectory r, continuously repeat 2-7.

More details on implementing the steps above on discrete approximation can be found in [36] and [37].

V. Results

A. Performance Results of Proposed Method for Simple Plant

First, a simple single-input, single-output (SISO) system under variable time-delay attack with a variable reference signal is considered. This test is conceived to demonstrate the usability and efficiency of the proposed method. The simulation model is given by

$$\dot{x}(t) = -0.7x(t) + 2u(t)$$
$$r(t) = \begin{cases} 1 - e^{-\gamma_2 t} & t \le T_a \\ 4e^{-\gamma_1(t-T_b)}(\sin(2\pi\omega_a t) + 1) & otherwise \end{cases} \quad (36)$$
$$\tau(t) = T_1 e^{-\lambda_1 t}(\sin(2\pi\omega_1 t) + 1) + T_2(1 - e^{-\lambda_2 t}) + 1$$

where the total simulation time T_{final}=500sec. T_a=T_{final}/2, T_b=T_{final}/2.2, T_1=T_2=T/10, λ_1=0.005, λ_2=0.0005, γ_1=0.07, γ_2=0.004, ω_a = 0.06, ω_1 = 0.005 and the sampling time is 0.01 sec.

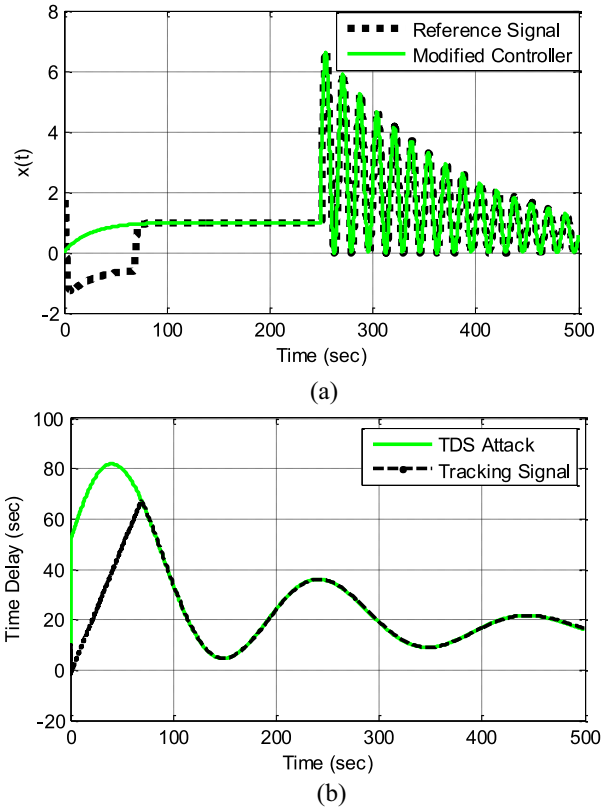
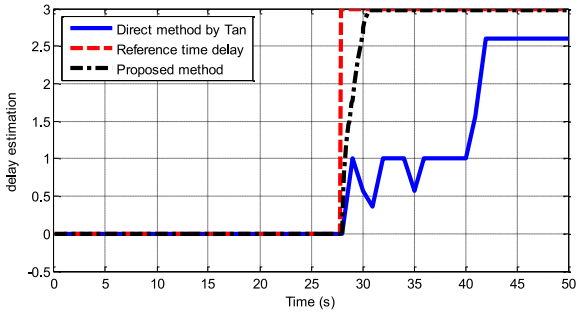


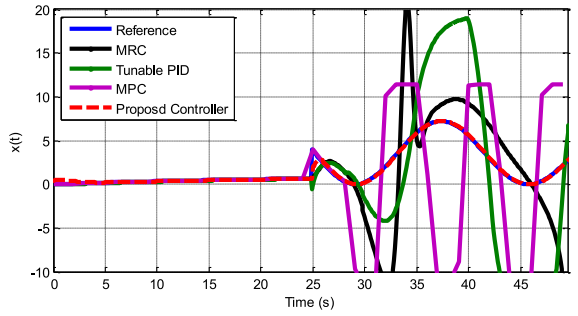
Fig. 3. (a) Tracking the performance of a single-input, single-output system under TDS attack. The dotted black line is the state of the system while green line is the reference signal. (b) Time-delay tracking. Dotted black line is time-delay estimate while green line is TDS attack.

The proposed PID controller was applied to track the reference signal under TDS attack. Figure 3(a) shows the state of the plant given in the Equation (32), tracking the desired trajectory $r(t)$. The tracking is almost perfect, even though the time delay varies by $\tau(t)$. Figure 3(b) shows the TDS attack detection and its tracking; the estimated time delay $\hat{\tau}(t)$ tracks the time-varying time delay $\tau(t)$ that can either be injected by an adversary or occurs naturally. Note that in the first 80 seconds of simulation. the plant's system operation does not track the reference signal because the time variable t is less than the time delay $\tau(t)$. In this plant simulation, a PID controller with the following parameters K_P=5, K_I=2 and K_D=1.5 was used. A Time-delay estimator learning rate η=0.32 was used, as well as a plant model teacher forcing effort parameter, C=2.

The simple modified model based on control and time-delay estimation has shown that it works for simple single- input,



(a)



(b)

Fig. 4. (a) The figure above illustrates that the time-delay estimation used by Tan [21] does not work well for the time-delay switch attack. A step time delay of 3sec, starting at 28sec, is applied to the system. The delay estimation using the direct method proposed by Tan is shown in blue. Red and black lines show the referenced time-delay attack; and time-delay estimation using the proposed method. While the neural network is attempting to estimate the time delay, it falls short of reaching the correct actual time-delay attack value. (b) Performance of the proposed method, compared with other time-delay control methods.

single-output systems under a complex variable time-delay attack.

B. Comparison to Other Time-Delay Estimation Methods

The model described in (36) was used for the purpose of comparisons with other methods, with some minor modifications in the sampling time, simulation time and TDS attack model. This modification was made for visualization purposes, as well as to make the attack model simpler. The methods selected were those with better performance.

The new TDS attack can be modeled as

$$\tau(t) = \begin{cases} 0 & t < 28 \\ 3 & t \geq 28 \text{ sec} \end{cases} \tag{37}$$

The total simulation time was set to T_{final}=*50sec,* and the sampling time to *0.01sec*.

The direct method time-delay estimation proposed by Tan [21] was applied to the proposed controller to show the performance of the proposed time-delay estimation method. The results in Figure 4(a) show that the proposed method tracks the step function TDS attack accurately in a shorter amount of time when compared with another method.

C. Comparison With Other Time-Delay Control Methods

We applied other control methods to control the system described in Equation (36) under TDS attack model described in Equation (37). These methods are the model referenced control (MRC), tunable PID controller (TPID) and model predictive controller (MPC). The methods used are part of the MATLAB Simulink package.

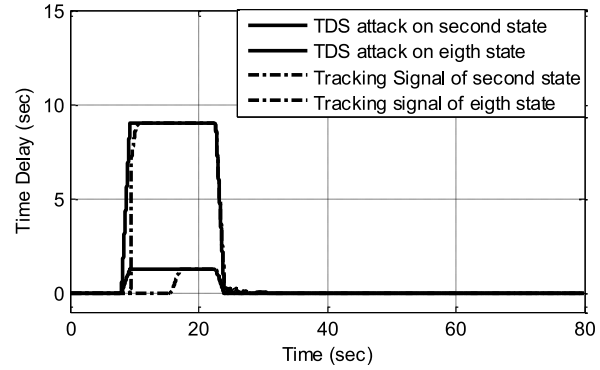
It should be noted that all of the controllers were designed in the most optimal way for possible TDS attacks.

The TPID, MRC and proposed controller were used with the following parameters *KP=5*, *KI=2* and *KD=1.5*.

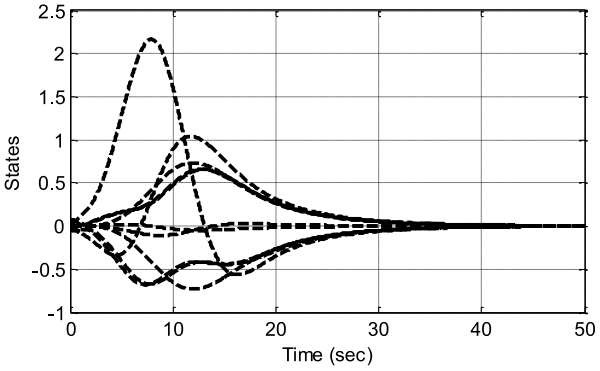
The TDS attack of 0.1s was applied from the starting time of 28 seconds to the system, and all of the controllers responded appropriately, with some methods responding better than others. Figure 4(b) shows the simulation results.

TABLE I
PARAMETER VALUES FOR A TWO-AREA POWER SYSTEM CONTROLLER DESIGN

Parameter	Value	Parameter	Value
J_1	10	ω_1	0.05
μ_1	1.5	T_{g1}	0.12 s
T_{tu1}	0.2 s	T_{tu2}	0.45 s
T_{12}	0.198 pu/rad	T_{21}	0.198 pu/rad
J_2	12	ω_2	0.05
μ_2	1	T_{g2}	0.18s
R	100I	Q_f	0
Q	100I	t_f	∞
β_1	21.5	β_2	21

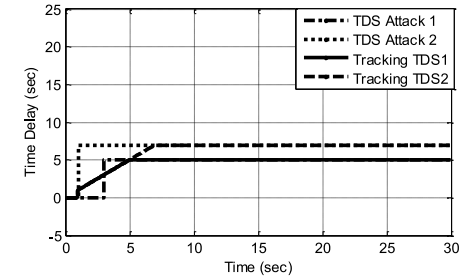


(a)

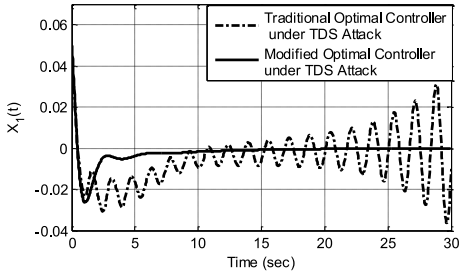


(b)

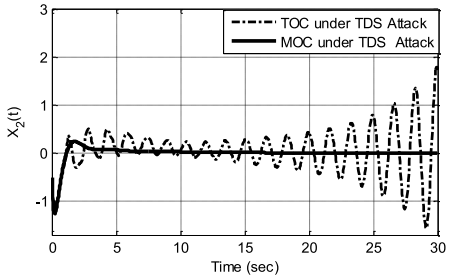
Fig. 5. (a) TDS attack tracking. (b) All states for the two-area LFC power system under TDS attack using the modified optimal controller. Initially, delays throw the system away from the stable point, however, shortly after time delays are estimated and the controller recovers, the regulating power states back to zero.



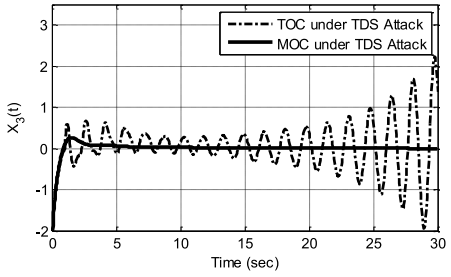
(a)



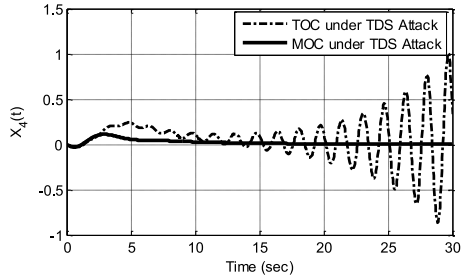
(b)



(c)



(d)

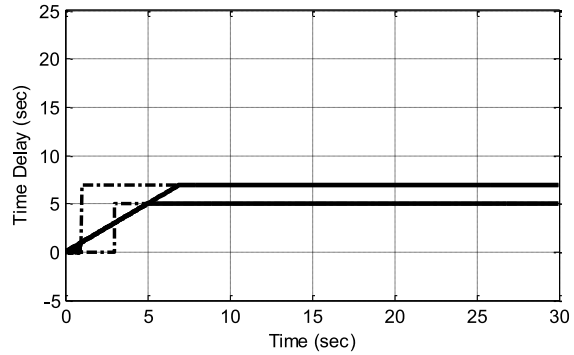


(e)

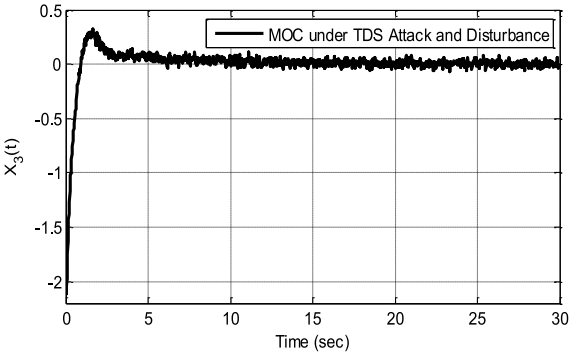
Fig. 6. (a) Time-delay tracking under TDS attack. (b) Frequency deviation, Δf^K. (c) Power deviation of generator, ΔP_g^K. (d) Value position of the turbine, ΔP_{tu}^K. (e) Tie-line power flow, ΔP_{pf}^1.

D. Performance Result of Proposed Method for LFC System

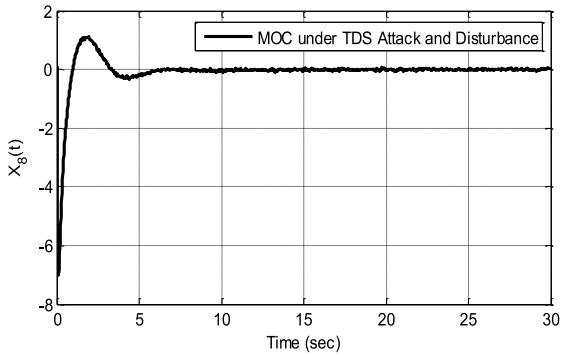
The distributed power control systems is where the time-delay mitigation strategies are paramount. The LFC system



(a)



(b)



(c)

Fig. 7. (a) TDS attack tracking. (b) Value position of the turbine system under TDS attack for the first power-area control system. (c) Value position of the turbine system under TDS attack for the second power-area control system.

(mentioned in Section II) is where the controller task regulates the state of a power plant network.

Simulation studies were conducted to evaluate the effects of TDS attacks on the dynamics of the system. By solving the Riccati matrix equation, the close loop control can be designed in the form of state feedback. For this simulation, a discrete linear-quadratic regulator design is used from the continuous cost function called the "lqrd" function in MATLAB 2013a. For simplicity of discussion, $N = 2$, which means a two-area power system.

Table I shows the parameter values used in this process. Since simulation for a certain duration tracks a step load change, both ΔP_l^1 and ΔP_l^2 zero are also set.

Scenario 1: The hacker injects time delays on the second and eighth states, from time 8s to 24s for a delay value of 1.28s and 9s respectively. The LFC system equipped with the

time-delay estimator performs well. Power states are being regulated to zero, and a TDS attack has been detected and time-delay tracked. Figure 5(a) shows the detection and tracking of the time delay, and Figure 5(b) shows all states for the two-area interconnected power system. As clearly shown from the figures, the modified controller was able to control the LFC distributed system under TDS attack.

Scenario 2: In this scenario, a TDS attack is injected at time 1s and 3s for delay values of 5s and 7s for the second and eighth states. Figure 6(a) shows that the tracking scheme works perfectly and could track the TDS attack. Figures 6(b), 6(c), 6(d) and 6(e) show the simulation results of frequency deviation, power deviation of the generator, value position of the turbine and tie-line power flow of the first power area, respectively with and without the modified control method. It shows that the system will be unstable under a TDS attack if the modified method is not applied. In figures 6(c) and 6(d) TOC and MOC denotes the traditional optimal controller and modified optimal controller, respectively.

Scenario 3: This scenario is exactly the same as the second scenario, except a 15 percent disturbance and noise was added to the system. As shown in Figure 7(a), the modified control technique could detect, track and control the LFC system under TDS attack, along with some disturbances. Figures 7(b) and 7(c) show the tracking performance of value position of the turbine system under TDS attack for the first and second power-area.

VI. Conclusion

It has been shown that the LTI systems can be controlled with variable time delays, either occurring naturally or as a result of a time-delay attack by a hacker. A TDS attack can also be successfully tracked with the proposed method. One kind of delay was addressed, that is, the delay in the observed state of the controlled system. In this paper, only the LTI system in state feedback was discussed. The method is general, and in the future papers, the method will be shown that it also works for a class of nonlinear systems.

References

[1] A. Sargolzaei, K. K. Yen, and M. N. Abdelghani, "Control of nonlinear heartbeat models under time-delay-switched feedback using emotional learning control," *Int. J. Recent Trends Eng. Technol.*, vol. 10, no. 2, pp. 85–91, 2014.

[2] C.-K. Zhang, L. Jiang, Q. H. 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.

[3] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.

[4] Q. Yang, D. An, and W. Yu, "On time desynchronization attack against IEEE 1588 protocol in power grid systems," in *Proc. IEEE Energytech*, Cleveland, OH, USA, May 2013, pp. 1–5.

[5] L. Schenato, "Optimal estimation in networked control systems subject to random delay and packet drop," *IEEE Trans. Autom. Control*, vol. 53, no. 5, pp. 1311–1317, Jun. 2008.

[6] M. S. Mahmoud, *Robust Control and Filtering for Time-Delay Systems.* New York, NY, USA: Marcel Dekker, 2000.

[7] H. J. Jia, X. D. Yu, Y. Yu, and C. Wang, "Power system small signal stability region with time delay," *Int. J. Elect. Power Energy Syst.*, vol. 30, no. 1, pp. 16–22, 2008.

[8] D. Dotta, A. S. e Silva, and I. C. Decker, "Wide-area measurements-based two-level control design considering signal transmission delay," *IEEE Trans. Power Syst.*, vol. 24, no. 1, pp. 208–216, Feb. 2009.

[9] I. Kamwa, R. Grondin, and Y. Hebert, "Wide-area measurement based stabilizing control of large power systems—A decentralized/hierarchical approach," *IEEE Trans. Power Syst.*, vol. 16, no. 1, pp. 136–153, Feb. 2001.

[10] H. X. Wu, K. S. Tsakalis, and G. T. Heydt, "Evaluation of time delay effects to wide-area power system stabilizer design," *IEEE Trans. Power Syst.*, vol. 19, no. 4, pp. 1935–1941, Nov. 2004.

[11] Q. Jiang, Z. Zou, and Y. Cao, "Wide-area TCSC controller design in consideration of feedback signals' time delays," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, vol. 2. San Francisco, CA, USA, 2005, pp. 1676–1680.

[12] M. S. Saad, M. A. Hassouneh, E. H. Abed, and A. A. Edris, "Delaying instability and voltage collapse in power systems using SVCs with washout filter-aided feedback," in *Proc. Amer. Control Conf.*, vol. 6. Portland, OR, USA, 2005, pp. 4357–4362.

[13] B. Chaudhuri, R. Majumder, and B. C. Pal, "Wide-area measurement-based stabilizing control of power system considering signal transmission delay," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, vol. 2. San Francisco, CA, USA, 2005, pp. 1447–1450.

[14] F. Milano and M. Anghel, "Impact of time delays on power system stability," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 59, no. 4, pp. 889–900, Apr. 2012.

[15] S. Ray and G. K. Venayagamoorthy, "Real-time implementation of a measurement-based adaptive wide-area control system considering communication delays," *IET Gener. Transm. Distrib.*, vol. 2, no. 1, pp. 62–70, Jan. 2008.

[16] S. Amin, A. A. Cardenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," paper presented at the Proc. 12th Int. Conf. Hybrid Syst. Comput. Control, San Francisco, CA, USA, 2009.

[17] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," paper presented at the 1st Workshop Secure Control Syst., Stockholm, Sweden, Apr. 2010.

[18] A. Sargolzaei, K. Yen, and M. N. Abdelghani, "Delayed inputs attack on load frequency control in smart grid," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. (ISGT)*, Washington, DC, USA, Feb. 2014, pp. 1–5.

[19] A. Sargolzaei, K. Yen, and M. N. Abdelghani, "Time-delay switch attack on load frequency control in smart grid," *J. Adv. Commun. Technol.*, vol. 5, pp. 55–64, Nov. 2014.

[20] S. Liu, X. P. Liu, and A. E. Saddik, "Denial-of-service (dos) attacks on load frequency control in smart grids," paper presented at the IEEE PES Innov. Smart Grid Technol. (ISGT), Washington, DC, USA, 2013.

[21] Y. Tan, "Time-varying time-delay estimation for nonlinear systems using neural networks," *Int. J. Appl. Math. Comput. Sci.*, vol. 14, no. 1, pp. 63–68, 2004.

[22] L. Chunmao and X. Jian, "Adaptive delay estimation and control of networked control systems," in *Proc. Int. Symp. Commun. Inf. Technol. (ISCIT)*, Bangkok, Thailand, Oct./Sep. 2006, pp. 707–710.

[23] N. Sadeghzadeh, A. Afshar, and M.-B. Menhaj, "An MLP neural network for time delay prediction in networked control systems," in *Proc. Control Decis. Conf. (CCDC)*, Yantai, China, Jul. 2008, pp. 5314–5318.

[24] A. Sargolzaei, K. K. Yen, S. Noei, and H. Ramezanpour, "Assessment of He's homotopy perturbation method for optimal control of linear time-delay systems," *Appl. Math. Sci.*, vol. 7, no. 8, pp. 349–361, 2013.

[25] M. T. Alrifai, M. Zribi, M. Rayan, and M. Mahmoud, "On the control of time delay power systems," *Int. J. Innov. Comput. Inf. Control*, vol. 9, no. 2, pp. 769–792, 2013.

[26] L. Jiang, W. Yao, Q. H. Wu, J. Y. Wen, and S. J. Cheng, "Delay-dependent stability for load frequency control with constant and time-varying delays," *IEEE Trans. Power Syst.*, vol. 27, no. 2, pp. 932–941, May 2012.

[27] M. Ma, H. Chen, X. Liu, and F. Allgöwer, "Distributed model predictive load frequency control of multi-area interconnected power system," *Int. J. Elect. Power Energy Syst.*, vol. 62, pp. 289–298, Nov. 2014.

[28] H. Bevrani, *Robust Power System Frequency Control*. New York, NY, USA: Springer, 2009.

[29] K. J. Åström and T. Hägglund, *Advanced PID Control*. Research Triangle Park, NC, USA: Inst. Syst. Autom. Soc., 2006.

[30] K. Zhou, J. C. Doyle, and K. Glover, *Robust and Optimal Control*, vol. 40. Upper Saddle River, NJ, USA: Prentice Hall, 1996.

[31] K. J. Åström and B. Wittenmark, *Adaptive Control*. Reading, MA, USA: Addison-Wesley, 2013.

[32] K. S. Narendra and A. M. Annaswamy, *Stable Adaptive Systems*. New York, NY, USA: Dover, 2012.

[33] S. Haykin, *Adaptiv Filter Theory*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1996.
[34] T. J. Lim and M. D. Macleod, "Adaptive algorithms for joint time delay estimation and IIR filtering," *IEEE Trans. Signal Process.*, vol. 43, no. 4, pp. 841–851, Apr. 1995.
[35] F. Reed, P. L. Feintuch, and N. J. Bershad, "Time-delay estimation using the LMS adaptive filter-static behavior; dynamic behavior," *IEEE Trans. Acoust. Speech Signal Process.*, vol. 29, no. 3, pp. 561–571, Jun. 1981.
[36] R. H. Middleton and G. C. Goodwin, *Digital Control and Estimation: A Unified Approach*. Englewood Cliffs, NJ, USA: Prentice Hall, 1990.
[37] W. J. Rugh, *Linear System Theory*, vol. 2. Englewood Cliffs, NJ, USA: Prentice Hall, 1996.

Arman Sargolzaei received the M.Sc. and Ph.D. degrees in electrical and computer engineering from Florida International University, Miami, FL, USA, in 2012 and 2015, respectively. He is a Faculty Member with the Department of Electrical and Computer Engineering, Florida International University. His research interests include control and power systems, telecommunications, and security of networked control systems and nonlinear systems. He has published over 25 journal and conference papers in the above areas. He is a part of Editorial Board and a Reviewer of several journal papers.

Kang K. Yen received the Ph.D. degree from Vanderbilt University in 1985. He is a Professor, the Graduate Program Director of the Electrical and Computer Engineering Department, and the International Program Development Director of the College of Engineering and Computing, Florida International University. His research interests include system modeling and simulation, advance control theory, signal processing, microprocessor, and AI applications.

Mohamed N. Abdelghani received the Master's degree in electrical and computer engineering from Southern Illinois University, and the first Ph.D. degree in neuroscience from the University of Toronto. He is currently pursuing the Ph.D. degree with the Department of Mathematics and Statistics, University of Alberta. His research interests include stochastic control, sensory motor control, and neural information processing.