IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 21, 2017, accepted July 14, 2017, date of publication July 27, 2017, date of current version August 29, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2731780

Resilient Design of Networked Control Systems Under Time Delay Switch Attacks, Application in Smart Grid

ARMAN SARGOLZAEI[1], (Member, IEEE), KANG K. YEN[2], (Senior Member, IEEE), MOHAMED N. ABDELGHANI[3], (Member, IEEE), SAMAN SARGOLZAEI[4], (Member, IEEE), AND BOGDAN CARBUNAR[5], (Member, IEEE)

[1]Department of Electrical Engineering, Florida Polytechnic University, Lakeland, FL 33805, USA
[2]Department of Electrical and Computer Engineering, Florida International University, Miami, FL 33199, USA
[3]Department of Mathematics and Statistics, University of Alberta, Edmonton, AB T6G 2R3, Canada
[4]Department of Neurosurgery, University of California Los Angeles, Los Angeles, CA 90095, USA
[5]School of Computing and Information Sciences, Florida International University, Miami, FL 33199, USA

Corresponding author: Arman Sargolzaei (a.sargolzaei@gmail.com)

ABSTRACT Industrial control systems are distributed hierarchical networks that share information via an assortment of communication protocols. Such systems are vulnerable to attacks that can cause disastrous consequences. This article focuses on time delay switch (TDS) attacks and shows that cryptographic solutions are ineffective in recovering from the denial of service component of TDS attacks. Therefore, a cryptography-free TDS recovery (CF-TDSR) communication protocol enhancement is developed that leverages adaptive channel redundancy techniques and a novel state estimator, to detect and recover from the destabilizing effects of TDS attacks. Simulation results are conducted to prove that CF-TDSR ensures the control stability of linear time invariant systems and to show the efficacy of CF-TDSR against attacks deployed on multi-area load frequency control components of a distributed power grid.

INDEX TERMS Power control systems, time-delay switch attack, attacks/faults tolerant designs, intrusion detection, adaptive communication channel, cyber attack, resilient design.

NOMENCLATURE

$x(t)$	State vector
$\hat{x}(t)$	State estimate vector
τ_{max}	Maximum time-delay allowed
$u(t)$	Control vector
e_m	Modeling error
β	Frequency bias factor
ΔP_l	Power deviation of the load
A	Constant matrix
B	Constant matrix
i, j	Power area indices
J	Generator moment of inertia
r(t)	Reference signal to be tracked
T_{tu}	Turbine time constant
K	The feedback optimal control gain
τ	Time delay in control design
Δf	Frequency deviation
e	Performance error
$\hat{e}$	Estimate of performance error
d	Time delay
ε	Error of the time delay estimation
ΔP_g	Power deviation of the generator
ΔP_{tu}	Position value of the turbine
ΔP_{pf}	Tie-line power flow
Λ	Control error
ω	Speed-droop coefficient
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
w	Zero-mean Gaussian white noise
μ	Expectation value
t_c	Time value of the clock maintained by the controller
t_s	Timestamp of the packet generated at the transmitter

I. INTRODUCTION

In recent years, the security of Networked Control Systems (NCSs) has raised many important research questions. NCSs, are used in modern power grids to monitor and control systems distributed over a wide area. This make modern power grid depend on computers and multi-purpose networks for operation, rendering them vulnerable to attacks, including high-profile cyber attacks [1]–[4], which have a potentially major societal impact.

This article focuses on Time Delay Switch (TDS) attacks on NCSs [5]–[7]. TDS attack, also called delay in service (DiS) attack causes delay into the transmission of measured signals from the plant output to the controller. Most communication algorithms have proposed the use of timestamps to address naturally occurring delays in the communication between plants and their controllers in the NCS [8], [9]. However, timestamping is not effective against TDS attacks, since the attackers can manipulate both the data and timestamps. TDS attack is new in nature but includes all other types of attack through the design and its framework. This helps researcher to focus on studying one type of attack instead of many others such as false data injection, jamming, denial of service attacks and many others.

Consider, for instance, a hacker that can manipulate both the data content and the timestamps of telemetered information (sensed from the output sensor). The data sent to the controller consists of a sequence of points of the form $(t, x(t))$, where $x(t)$ denotes the state of the plant at time t. The attacker can modify this data in one of several ways. First, manipulate the timestamps, i.e., send $(t - d, x(t))$, where d is a random positive delay. Second, delay the state values, i.e., send $(t, x(t - d))$. Third, change both the timestamp and the data, i.e., send $(t - d_1, x(t - d_2))$, where d_1 and d_2 are random positive delays. Finally, the attacker can simply drop the packets which will cause delay in service.

Cryptographic solutions may be used to detect some attacks. For instance, the packets can be authenticated, e.g., using keyed hashes (e.g., a keyed-hash message authentication code (HMAC)), and computed using a key shared only by the controller and the plant. Even if the cryptographic constructs are fast and will introduce only small delays and computing overhead, they are unable to recover from denial of service (DoS) type of TDS attacks, or to recover data delayed or destroyed by the hacker since controller needs data at the time it expect them. If packets which have most powerful cryptographic constructs received by delay or dropped in the line then controller might be able to detect it but cannot recover them at the time that controller needs them. The controller will be forced to request the retransmission of the lost or corrupt packets, leading to additional delays and a higher network load that can destabilize the entire system.

In this article, the adaptive channel allocation techniques are leveraged, along with state predictors and time-delay detectors to address the challenges introduced by TDS attacks. Adaptive resource allocation techniques and channel adaptive methods provide substantial improvements and robust performance under many benchmarking metrics [10]. These methods employ an adaptive communication resources allocation as the channel conditions change by time [11]. More information about adaptive resource allocation techniques can be found in [10]–[12].

The contribution of this paper is listed here: 1- Formulating and introducing TDS attack to cover several different types of existing attacks. 2- Introducing a Crypto-Free TDS Recovery (CF-TDSR) protocol ensure reliability and security of control systems while minimizing cost of redundant communication channels. CF-TDSR is a novel solution that requires the controller to first compare the received packet against an internally generated one and then adapt itself and communication channel. CF-TDSR protocol requires time synchronization between the plant and the controller. If a discrepancy is detected, then the telemetered information is discarded and the controller uses a predicted state, generated by a state predictor. If the data is delayed, the controller compares the value of the measured states against an internally predicted state and in the case that the difference exceeds a predetermined threshold, the controller drops the packet and uses the estimated state instead. In both cases, the controller sends a command signal to the data measurement unit to transmit the next data sets over multiple channels.

The article is structured as follows. Section II describes related work. In Section III, the system and adversary model, including TDS attacks are provided. Then, the paper introduce the load frequency control (LFC) system and use the adaptive allocation method to demonstrate mechanisms to restore stability after a time delay attack. The following section studies the TDS attack as a DoS attack. Section V, introduces CF-TDSR protocol, and demonstrates that CF-TDSR can eliminate the effects of TDS attacks. Section VI presents simulation results, and Section VII is the conclusion and recommendations.

II. RELATED WORK

The control of power systems with time delays has been previously explored [1], [2], [13]–[17]. Researchers, however, considered either the construction of controllers that are robust to time delays or controllers that use offline estimation. At this time, it seems to be no control methods and adaptive communication protocols that implement an online estimation of dynamic time delays and real-time control of power systems to overcome TDS attacks.

The stability of power control systems with time delays was studied in [18]–[22]. The author of [23] studied the stability effects of delays to the power systems. References [18] and [19] proposed methods to reduce oscillations resulting from time-delayed feedback control. Paper [24] introduced a wide-area control system for oscillations of a generator. Based on phasor measurements with delays, a novel controller was suggested in [17] where the power system's small signal stability was considered. Reference [25] proposed a controller for power systems with

delayed states. The controller addresses the effects of delayed states using the quadratic Lyapunov function.

Related work on time-delay estimation includes [26]–[29]. In [26], the author suggested a neural network approach to estimate time delays for a class of nonlinear systems with time-varying delays. Li in [27] developed an adaptive control procedure to estimate random time delays in NCSs. This algorithm updates the time-delay estimation via gradient descent method, and determines plant parameters by an enhanced recursive least square. However difficulties may arise from the complexity of this solution, even for simple linear systems. In [28], the authors used a multilayer perceptron neural network to estimate the time delay off-line. This method assumes a constant time delay or one that follows a specific pattern. With this assumption, this solution is harder to apply to TDS attacks. A new resilient control method for systems under TDS attack, which can estimate the TDS attack in real time and overcome its effects was proposed in [30]. However, it doesn't adapt the communication channels to overcoming and preventing future attacks. In this paper, a new CF-TDSR protocol to detect the attack in real time and adapt the communication channels while adapting the controller to overcoming and preventing the current and future TDS attacks is developed.

III. SYSTEM AND ADVERSARY MODEL AND BACKGROUND

The following section introduces the system and adversarial model used to validate CF-TDSR protocol. Background information of this research is also discussed.

A. SYSTEM MODEL UNDER TDS ATTACK

Figure 1 illustrates a two-area power plant with automatic generation control (AGC). The LFC component sends control signals to the plant and receives state feedback through the communication channel. Different attack types can be launched against an LFC system, including DoS, False Date Injection (FDI) and Time Delay Switch (TDS) [6] attacks.

The LFC is a large scale NCSs that regulates the power flow between different areas while holding the frequency constant. Power systems are usually large-scale systems with complex nonlinear dynamics. Modern power grids are divided into various areas. Each area is connected to its neighboring areas by transmission lines called tie-lines. Tie-lines facilitate power sharing between neighboring areas. LFC is used to make sure the power grid is stable and efficient. Furthermore, analysis of power generation and control systems' markets showed that LFC plays an important role as one of the most profitable supporting service in these systems that provide better conditions for electricity trading [31]. More information about technical part of LFC can be found in [32], [33].

LFCs are usually designed as optimal feedback controllers. In order to operate on an optimal level, the LFC requires power state estimates to be telemetered in real time. In the case when an adversary injects TDS attack to the telemetered

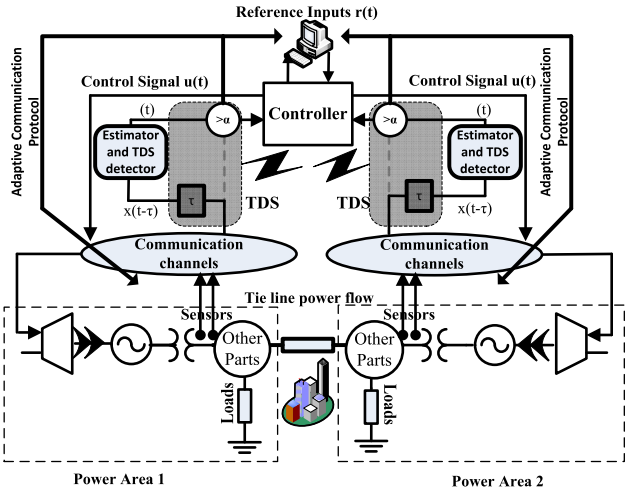

FIGURE 1. Two-area power system controlled under TDS attack, Each power area is separated by dashed lines which contain turbines, generator and loads. Sensors in each power area measure the output state and send them to centered LFC. The feedback line sends sensor data through communication channels where, the TDS attacks takes place. Obviously, other types of attack are possible on the communication lines.

control signals or communication channel of feedback loop, the LFC will diverge from its optimality, and in most cases, depending on the amount and duration of the attack. The system will even get unstable if there is no prevention and stabilizer are in place such as our proposed protocol. In [6], [7], an LFC power system under TDS attacks is modeled as a hybrid system. The LFC multi-area interlock power system has been explained in [6], [7]. Consider the multi-area LFC power system with the attack model, as follows:

$$\begin{cases} \dot{X}(t) = AX(t) + BU(t) + D\Delta P_l \\ X(0) = X_0 \end{cases} \tag{1}$$

where ΔP_l is the power deviation of the load. The optimal feedback controller can be found as

$$U = -K\hat{X} \tag{2}$$

and the new state after the time delay attack is given by

$$\hat{X}(t) = X(t - \tau) \tag{3}$$

where $\tau = [t_{d1}, t_{d2}, \ldots, t_{dN}]^T$ are different/random positive value time delays and t is time vector which is the same for all states.

While the system is in its normal operation, $t_{d1}, t_{d2}, \ldots, t_{dN}$ are all zero. An adversary can get access to the communication channel or sensors and add delays to the channel to make the system unstable. In (1), $X = [x_1, x_2, \cdots, x_N]^T$ denotes the states in each power area.

The state vector in the i^{th} power area is described as

$$x_i(t) = [\ \Delta f^i(t)\ \Delta P^i_g(t)\ \Delta P^i_{tu}(t)\ \Delta P^i_{pf}(t)\ \Lambda^i(t)\ ]^T \tag{4}$$

where Δf^i, ΔP^i_g, ΔP^i_{tu}, ΔP^i_{pf} and Λ^i are the frequency deviation, the power deviation of the generator, the position value of the turbine, the tie-line power flow, and the control

error on the i^{th} power area, respectively [22]. The control error of the i^{th} power area is expressed as

$$\Lambda^i(t) = \int_0^t \beta_i \Delta f^i(s) dt \tag{5}$$

where β_i denotes the frequency bias factor.

The dynamic model of the multi-area LFC of (1) can be expanded using

$$A = \begin{bmatrix} A_{11} & A_{12} & A_{13} & \cdots & A_{1N} \\ A_{21} & A_{22} & A_{23} & \cdots & A_{2N} \\ A_{31} & A_{32} & A_{33} & \cdots & A_{3N} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_{N1} & A_{N2} & A_{N3} & \cdots & A_{NN} \end{bmatrix} \tag{6}$$

$$B = diag\{\begin{bmatrix} B_1^T & B_2^T & B_3^T & \cdots & B_N^T \end{bmatrix}^T\} \tag{7}$$

$$D = diag\{\begin{bmatrix} D_1^T & D_2^T & D_3^T & \cdots & D_N^T \end{bmatrix}^T\} \tag{8}$$

where A_{ii}, A_{ij} B_i and D_i are represented by

$$B_i = \begin{bmatrix} 0 & 0 & \frac{1}{T_{gi}} & 0 & 0 \end{bmatrix}^T \tag{9}$$

$$A_{ij} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -2\pi T_{ij} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{10}$$

$$A_{ii} = \begin{bmatrix} -\frac{\mu_i}{J_i} & \frac{1}{J_i} & 0 & -\frac{1}{J_i} & 0 \\ 0 & -\frac{1}{T_{tu\,i}} & \frac{1}{T_{tu\,i}} & 0 & 0 \\ -\frac{1}{\omega_i T_{g\,i}} & 0 & -\frac{1}{T_{g\,i}} & 0 & 0 \\ \sum_{\substack{i \neq j \\ j=1}}^{N} 2\pi T_{ij} & 0 & 0 & 0 & 0 \\ \beta_i & 0 & 0 & 0 & 1 \end{bmatrix} \tag{11}$$

and

$$D_i = \begin{bmatrix} -\frac{1}{J_i} & 0 & 0 & 0 & 0 \end{bmatrix}^T \tag{12}$$

Here N denotes the number of power areas, J_i, ω_i, μ_i, $T_{g\,i}$, and $T_{tu\,i}$ are the generator moment of inertia, the coefficient for droop speed, coefficient for generator damping, the time constant of governor, the time constant of turbine in the i^{th} power area, and T_{ij} is the tie-line synchronizing coefficient between the i^{th} and the j^{th} power areas, respectively.

B. THE TIME DELAY ATTACK

To describe the TDS attack, a simplified version of Figure 1 is shown in Figure 2. The plant (P) sends state variables, $x(t)$ as information packets to the controller (C). The state variables $x(t)$ are compared with reference inputs $r(t)$, to produce the error value $e(t) = r(t) - x(t)$. The error values are injected into the controller to calculate the control signals $u(t)$. This paper assumes that all packets sent by controller include data and timestamps (either encrypted/authenticated, or not). Also, for simplicity, it is assumed that the attacker can only target the communication channel between the plant and the controller. The attacker can launch the different TDS attack, as follows:

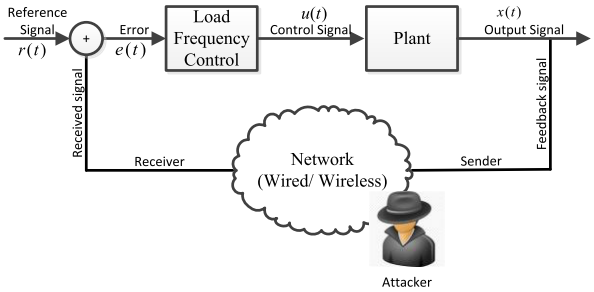

FIGURE 2. A simplified LFC system under TDS attack. The plant is a power area system controlled by the LFC. $x(t)$ is a vector of the power area states. $x(t)$ is measured and transmitted to the controller via communication links. u(t) is the control signals. $r(t)$ is the desired state and e(t) is the difference between desired state and measured plant state. The attacker attacks the communication link between the plant and controller either by dropping the packets or delaying them.

1) REPLAY-BASED TDS ATTACK

The attacker leaves the first message $x(0.1)$ intact. It then records but drops the second message, $x(0.2)$, and resends the first massage again. Subsequently, it sends $x(0.2)$ instead of the third message, etc. The attacker can generalize this attack by introducing different time delays. The control input (error signal) under 0.1 seconds of delay will be $r(0.2) - x(0.1)$ or $r(0.2)$ in the case that receiver detects the attack or fault. Table 1 illustrates the steps of this attack where the attacker is added delay of 0.1 seconds. In the table 'TS' denotes timestamp.

TABLE 1. Sequence of events during a replay TDS attack.

TS	*{TS, P(t)}*	*{TS, C(t)}*	*Controller Input(* e(t) *)*
0.1	$\{0.1, x(0.1)\}$	$\{0.1, x(0.1)\}$	$e(t) = r(0.1) - x(0.1)$ or $e(t) = r(0.1) - 0$
0.2	$\{0.2, x(0.2)\}$	$\{0.1, x(0.1)\}$	$e(t) = r(0.2) - x(0.2 - 0.1)$ or $e(t) = r(0.2) - 0$
0.3	$\{0.3, x(0.3)\}$	$\{0.2, x(0.2)\}$	$e(t) = r(0.3) - x(0.3 - 0.1)$ or $e(t) = r(0.3) - 0$

2) TIMESTAMP-BASED TDS ATTACK

The attacker reconstructs the packet and fixes the timestamp. Subsequently, the timestamping detector will not be able to find the time delay attack.

The attacker receives the first message from the plant and copies the value in the buffer, then substitutes the state value of the first packet inside the second message and reconstructs the packet. Then, the adversary sends the packet to the controller. Table 2 illustrates this attack scenario. In this table, x_1 denotes the first state value, x_2 is the second one and so forth.

TABLE 2. Sequence of events during timestamps alter TDS attack.

TS	*{TS, P(t)}*	*{TS, C(t)}*	*Controller Input* (e(t))
0.1	$\{0.1, x_1(0.1)\}$	$\{0.1, x_1(0.1)\}$	$e(t) = r_1(0.1) - x_1(0.1)$
0.2	$\{0.2, x_2(0.2)\}$	$\{0.2, x_1(0.1)\}$	$e(t) = r_2(0.2) - x_1(0.2)$ $= r_2(0.2) - x_2(0.2-0.1)$
0.3	$\{0.3, x_3(0.3)\}$	$\{0.3, x_2(0.2)\}$	$e(t) = r_3(0.3) - x_2(0.3)$ $= r_3(0.3) - x_3(0.3-0.1)$

Let's say the plant sends x_2 at time 0.2, and the attacker copies the state value (packet). Now consider that the controller gets x_3, at time 0.3. During this time attacker sends x_2 instead of x_3 with a corrected 0.3 timestamp. This can occur even in encrypted scenarios if the attacker can decrypt the packet and reconstruct it with a new wrong state and correct timestamps. as shown in Table 2.

3) NOISE-BASED TDS ATTACK

The attacker injects fake packages into the system, making the system delay the transmission of system packages. Also temporally communication channel jamming can be classified as this type of attack. This way, the packets of the plant are delivered to the controller with a delay.

In all the above variants, the attacker injects time delays into the control system, making the system unstable or inefficient, as was shown in [6].

IV. TDS ATTACK AS A DENIAL-OF-SERVICE (DoS) ATTACK: A UNIFIED APPROACH

In this section, a unified approach to model a special case of TDS attacks as DoS attacks is proposed. Then, techniques will be investigated that address TDS attacks. Consider a linear time invariant (LTI) system described as

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) + w(t) \\ u(t) &= -Kx(t) \end{aligned} \tag{13}$$

where $x \in R^n$ and $u \in R^m$ are state and control signals, respectively. Matrices A, B and K are constant which have appropriate dimensions. The vector $w \in R^n$ is an n-dimensional zero-mean Gaussian white noise process. Suppose that a TDS attack occurs with probability p. Then

$$\dot{x}(t) = \begin{cases} (A - BK)\,x(t) + w(t) & 1-p \\ Ax(t) - BKx(t-\tau) + w(t) & p \end{cases} \tag{14}$$

where p is probability of TDS attack occurrence and 1-p is probability that system is in normal operation.

To simplify this explanation, in (14) we assume that the same probability of attack occurs on different channels and states. If a TDS attack occurs and packets are dropped, then, (14) is formulated in the form of a DoS attack as follows

$$\dot{x}(t) = \begin{cases} (A - BK)\,x(t) + w(t) & 1-p \\ Ax(t) + w(t) & p \end{cases} \tag{15}$$

Let us calculate the expectation value of $\dot{x}$ in (15) as:

$$\begin{aligned} E\{\dot{x}(t)\} = \begin{bmatrix} (A - BK)\,E\{x(t)\} \\ +E\{w(t)\} \end{bmatrix} (1-p) \\ + \left[AE\{x(t)\} + E\{w(t)\}\right] p \end{aligned} \tag{16}$$

Let $\mu(t) = Ex(t)$, then one can write (16) as

$$\begin{aligned} \dot{\mu}(t) &= \left[(A - IBK)\,\mu(t)\right](1-p) + A\mu(t)p \\ &= (A - (1-p)BK)\,\mu(t) \end{aligned} \tag{17}$$

where $Ew = 0$. Next, the stability of (17) is investigated. In order for the system described in (17) to be stable, the mean should be bounded. Therefore, this equation must satisfy:

$$\{A - (1-p)BK < 0\} \tag{18}$$

Hence,

$$A - BK + pBK < 0 \tag{19}$$

i.e., $A - Bk + pBK$ must be negative definite for the system to be stable. If there is no attack on the system, then the following condition can be found:

$$A - BK < 0 \tag{20}$$

To satisfy the stability requirement, condition (19) must be made as close as possible to (20). To achieve this, two possibility are available. First, the probability of a TDS attack on the communication channel is decreased. Second, the controller gain is changed. In the following probability equations, both cases are described.

A. DECREASING PROBABILITY OF TDS ATTACK

In this case, the outcome of an attack is investigated when the protocol resends each packet l times over independent channels. Then, the probability a TDS attack decreases by power l, i.e.,

$$\dot{x}(t) = \begin{cases} (A - BK)\,x(t) + w(t) & 1 - p^l \\ Ax(t) + w(t) & p^l \end{cases} \tag{21}$$

Equation (19) will take the form

$$A(BK)^{-1} - I + (pI)^l < 0 \tag{22}$$

Therefore

$$\begin{aligned} A(BK)^{-1} - I &< A(BK)^{-1} - I + (pI)^l \\ &< A(BK)^{-1} - I + pI < 0 \end{aligned} \tag{23}$$

The condition in (23) shows that if $l > 1$ channel is allocated to increase the redundancy of transmitted plant data, the total probability of faults will decrease as a result of a TDS attack. Also, the control system will get closer to its original state, i.e., $A - BK < 0$. Therefore, by adaptively adding another communication channel(s), the LFC system can be stabilized. The cost of channel redundancy limits the number of communication channels that can be added to address TDS attacks. The alternative is to change the controller gain.

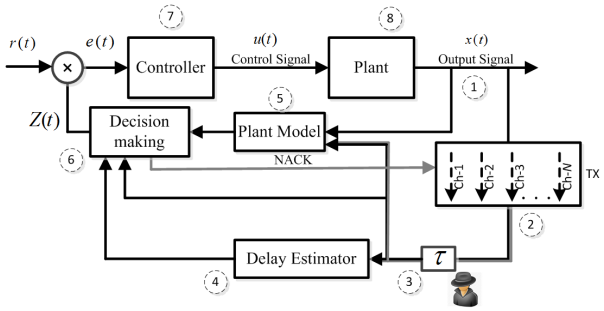

FIGURE 3. Block diagram of CF-TDSR. Tx is the plant transmitter of measured data. Tx receives as it inputs a signal from the delay detector if a time-delay attack is detected. The Delay Estimator unit continuously estimates the time delays in the communication link. The delay Detector, or more appropriately, the adverse delays detector, receives a signal from the plant estimator and delay estimator and makes a decision whether or not to inform the transmitter to request multiple redundant channels. The plant model estimates the plant state continuously. The controller produced the required control signals to stabilize the plant.

B. CHANGING CONTROLLER GAIN

Changing the controller gain K to stabilize the NCS is proposed along with the first method. The new controller gain parameter is set to be $K_p = K/(1-p)$. In this case, a limited number of channels only need to be added. However, adjusting the controller gain K is subject to the probability of attack p which is difficult to estimate. This control methodology is described in detail in section VI.

V. CF-TDSR: A CRYPTO-FREE TDS RECOVERY PROTOCOL

In this section, the CF-TDSR, a communication and control protocol that thwarts TDS attacks on NCSs is introduced. The CF-TDSR leverages methods to detect different types of TDS attacks introduced by a hacker. It also compensates negative effects of attacks on system. The CF-TDSR consists of the following components (see Figure 3 for the system diagram). First, the smart data transmitter (Tx) adaptively allocates transmission channels on demand. Second, the plant model estimates the current plant states and helps to stabilize the system under attack. Third, the time-delay estimator continuously estimates time delays on the channels. Fourth, the time-delay detector and decision making unit (DMU) that determines if delays are detrimental to the system. The DMU also detects faults and other types of attacks such as FDI accordingly. In this case, it will issue commands to inform the transmitter and controller. The last component is the controller to control the system (controller block in Figure 3). The τ block in the diagram represents a hacker which injects TDS attack to the communication channels. The adversary can inject other types of attacks as well. The CF-TDSR protocol works as follows:

State variables ($x(t)$) are sensed using sensors (point 1 in the diagram) and will be sent to the transmitter (Tx) unit (point 2). The transmitter unit constructs the packet and allocates the communication channel and transmits the packet to the delay estimator and plant model unit. The TX unit can transmit the constructed packet through one channel or more. The attacker can inject the TDS attack to the communication channel after packets are sent from transmitter unit (point 3). Plant model calculates the estimated states (point 5) and send it to DMU. The amount of delay will be estimated using delay estimator unit at the same time (point 6). The DMU (point 6) receives the estimated states along with delay estimate and based on pre-defined rules make a decision to whether request a new redundant channel or not. It also informs the controller (point 7) to adapt itself under attack until receiving the next healthy packet. The controller generates the control signal and sends it to the plant (point 8). The CF-TDSR will detect and track time delays introduced by a hacker and guide the plant to track the reference signal to improve the system performance.

The CF-TDSR is flexible and is able to support communication between the plant and the controller with and without timestamps. In the case where timestamps are used, the controller compares the controller clock and the packet timestamp and the state of the plant with the state predicted by the plant model. If there are any differences, the packet is dropped. If this is the case, the controller sends a negative acknowledgment (NACK) signal to the communication transmitter to use an adaptive channel allocation. Finally, the controller uses the state predicted by the plant model instead of the state received in the packet to control the system while it waits for the corrected future packets.

In the case where timestamps are not used, the time delay estimator continuously estimates time delays, while the plant model determines the appropriate plant state values. If the estimated time delays are larger than the tolerable time delay, or if the plant state estimates are different from the received plant states, the communicated packet is dropped. Similar to the previous case, in this case, the DMU unit signals the communication transmitter to use adaptive channels allocation and its internal state estimates for control purposes.

A. DECISION-MAKING UNIT (DMU)

The functionality of the delay detector which is part of DMU unit can be captured with the following mathematical formula:

$$D(t) = \begin{cases} 1 & (|t_c - t_s| > \tau_{stable}) \quad or \quad (|e_m(t)| > \varepsilon) \\ & or \quad \left(\hat{\tau} \geq \tau_{stable}\right) \\ 0 & otherwise \end{cases} \tag{24}$$

where $D(t)$ is the detection function, t_c is the time value of the clock maintained by the controller, t_s is the timestamp of the packet generated at the transmitter, and τ_{stable} is the tolerable time delay, or the maximum time delay for which the system remains in the stable region. This can be calculated from the eigenvalues of the system, as shown in [4]. Here, $e_m(t) = x(t) - \hat{x}(t)$ is the difference between the transmitted state of the plant $x(t)$ and the plant estimator record of the system state, $\hat{x}(t)$, and ε is the maximum tolerable error value. Since TDS attacks occur with probability p, then $D = 1$ with probability p and $D = 0$ with probability $1 - p$ can

occur. Equation (24) enables the detection of TDS attacks and other types of attacks such as FDI irrespective of the use of timestamps, even if the timestamps are modified by the hacker.

The DMU generates the $Z(t)$ signal based on pre-defined rules. The $Z(t)$ can be estimated state or received state value regardless if its faulty or not. This would address other types of attacks in the system such as FDI attack. Due to this feature of DMU, two types of CF-TDSR protocol will be presented. The first type only detects the TDS and other types of attacks and only sends an NACK signal to the transmitted to request an additional redundant communication channel which is called "CF-TDSR-Type1" and the second type benefits with both adaptive communication channel and controller by sending an NACK to the transmitter along with sending estimated state to the controller to adapt it, called CF-TDSR-Type2. While CF-TDSR-Type2 is more accurate and cost efficient, type 1 is more applicable to highly nonlinear and complex systems.

B. DELAY ESTIMATOR UNIT

Consider a system that can be approximated in a region of interest by an LTI system. Equation (13), without the noise term, can be described by

$$\dot{x}(t) = Ax(t) + Bu(t) \tag{25}$$

The solution of this equation is

$$x(t) = e^{At}x_0 + \int_0^t e^{A(t-s)}Bu(s)ds \tag{26}$$

Given a time delay τ, introduced by a TDS attack or by natural causes, the solution becomes

$$x(t-\tau) = e^{A(t-\tau)}x_0 + \int_0^{t-\tau} e^{A(t-\tau-s)}Bu(s)ds \tag{27}$$

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

$$e_m(t;\tau,\hat{\tau}) = x(t-\tau) - \hat{x}(t-\hat{\tau}) \tag{28}$$

The idea is to estimate $\hat{\tau}$ in time as fast as possible to minimize the modeling error $e_m(t;\tau,\hat{\tau})$. To do so, let us assume $v = e_m^2/2$. The equation that minimizes the error is given by

$$\frac{d\hat{\tau}}{dt} = -\eta\frac{\partial v}{\partial \hat{\tau}} \tag{29}$$

where η is the learning parameter to be determined in conjunction with the PID or the optimal controller coefficients.

Then

$$\begin{aligned}\frac{d\hat{\tau}}{dt} &= -\eta\frac{\partial v}{\partial \hat{\tau}} = -\eta e_m\frac{\partial e_m}{\partial \hat{\tau}}\\ &= -\eta e_m\left[Bu(t-\hat{\tau}) - e^{A(t-\hat{\tau})}Bu(0) - Ae^{A(t-\hat{\tau})}x_0\right]\end{aligned} \tag{30}$$

In this paper, we assume $u(0) = 0$ at the initial time. Then,

$$\frac{d\hat{\tau}}{dt} = -\eta\, e_m Bu(t-\hat{\tau}) - Ae^{A(t-\hat{\tau})}x_0, \quad 0 \le \hat{\tau} \le t \tag{31}$$

Equation (31) is used to estimate the time delay τ. This process has some practical issues that should be considered. Computing machines have temporal resolution and finite memory. Therefore, (31) cannot be implemented without appropriate discrete approximation and boundedness assumptions. To assure the calculations stability and limit the memory usage, the following condition should be added, $\tau < \tau_{\max}$. This condition will create a finite buffer to store the history of $u(t)$ from t to $t - \tau_{\max}$ and also to prevent a runaway condition on $\hat{\tau}$.

In the following section, a novel method to prevent TDS attacks on LFC systems is illustrated.

C. PROOF OF STABILITY FOR THE LFC UNDER TDS ATTACK

Consider a power area LFC system of the form

$$\dot{x}(t) = Ax(t) + Bu(t) + w(t) \tag{32}$$

with the optimal controller given by

$$u(t) = -K\hat{x}(t) = \begin{cases} -Kx(t) & 1 - D(t) \\ -K\hat{x}(t) & D(t) \end{cases} \tag{33}$$

where $D(t)$ is a digital random process. $D(t)$ is 1 when a TDS attack is detected (see (24)) and is zero otherwise. TDS attacks are detected by comparing the received timestamp from the plant against the controller time, or by using the time-delay estimator; (see (31)). The new state estimate, $\hat{x}(t)$, is given by

$$\dot{\hat{x}}(t) = \begin{cases} Ax(t) + Bu(t) & 1 - D(t) \\ A\hat{x}(t) + Bu(t) & D(t) \end{cases} \tag{34}$$

Let the estimation error be $e_m(t) = \hat{x}(t) - x(t)$. The dynamics of the closed loop can be described as

$$\dot{x}(t) = \begin{cases} (A - BK)\,x(t) + w(t) & 1 - D(t) \\ & \text{and } e_m(t) = 0 \\ (A - BK)x(t) - BKe_m(t) + w(t) & D(t) \end{cases} \tag{35}$$

Now, let us investigate the stability of (35). For a reasonable stability criteria and for the covariance of $e_m(t)$ to remain bounded, the mean of the estimation error $e_m(t)$ should converge to zero. If $e_m(t)$ is bounded the covariance, then it has convergence for state $x(t)$. The total expectation value is computed over both $x(t)$ and $D(t)$, knowing that $D(t) = 1$ with probability p when there is an attack on one

channel. Thus, the equation of the system under attack can be expressed as

$$\dot{x}(t) = \begin{cases} (A - BK)\, x(t) + w(t) & 1 - p \\ (A - BK)x(t) - BKe_m(t) + w(t) & p \end{cases} \quad (36)$$

Therefore, the total expectation yields:

$$\begin{aligned} \dot{\mu}(t) &= (A - BK)\mu(t)(1 - p) \\ &\quad + (A - BK)\mu(t)p - BK\,\mu_m(t)p \\ &= (A - BK)\mu(t) - BK\,\mu_m(t)p \end{aligned} \quad (37)$$

Let us now assume that l channels are added to the communication channel:

$$\dot{\mu}(t) = (A - BK)\mu(t) - BK\,\mu_m(t)p^l \quad (38)$$

If the term $BK\,\mu_m(t)p^l$ approach to zero, (38) will converge to zero and the system will be stable. Therefore, the idea is to make that term as small as possible by choosing a large l or by using a good estimator for the system that can make this term closer to zero or bounded.

If the delay injected by the attacker exceeds $\tau_{\max}$, a trap condition signal is sent to the supervisory control and data acquisition (SCADA) center. The controller switches to open loop control until problem gets solved.

VI. SIMULATION RESULTS

Simulations are conducted to evaluate the performance of CF-TDSR protocol under TDS attacks. The discrete linear-quadratic regulator design from the ''lqrd'' continuous cost function (MATLAB 2013a) is used to generate the optimal control law for the system in normal operation. The two-area power systems are modeled, as described in Section IV. Table 3 shows the parameter values used in the simulation, based on literature [1], [2], [6]. Also, ΔP_l^1 and ΔP_l^2 is set to zero.

TABLE 3. Parameter values for a two-area power system with optimal controller [32].

Parameter	Value	Parameter	Value
$J_1(s)$	$10s$	ω_1	0.05
μ_1	1.5	T_{g1}	$0.12s$
$T_{tu\,1}$	$0.2\,s$	T_{tu2}	$0.45s$
T_{12}	$0.198\ pu\ /\ rad$	T_{21}	$0.198\ pu\ /\ rad$
$J_2(s)$	$12s$	ω_2	0.05
μ_2	1	$T_{g\,2}$	$0.18s$
R	$100I$	Q_f	0
Q	$100I$	t_f	∞
β_1	21.5	β_2	21

The goal of the simulation is to demonstrate the ability of the CF-TDSR to quickly respond to the TDS attacks. The total simulation time is set to 50 seconds. The example assumes that a hacker has access to the communication channel. The attacker starts the TDS attack with values of $\tau = \left[t_{d1}\ t_{d2} \cdots t_{dn}\right]^T$. Each power area has five states. Since a two-area power system is considered, the total number of states in the interconnected model is 10. Consider that the attack starts at time t_a.

The simulation is performed in three main scenarios: composite TDS attack, single power plant attack, and simultaneous composite TDS attack on a noisy system and limited available channel.

A. COMPOSITE TDS ATTACK

In the first investigation, a case is simulated where a hacker attacks the third state of both power areas. Since the third state of each area provides the feedback, it is thus an ideal place for the TDS attack. We assumed that there is only one extra channel available to allocate in this scenario. The attack starts at $t_a = 1\,s$ for the first power area and at $t_a = 3s$ for the second power area, with time-delay injected values of $t_{d3} = 1.5s$ (time delay associated to third state of first plant) and $t_{d8} = 3s$, respectively. Figure 4(a) illustrates the TDS attack and their tracking using our proposed delay estimator unit. In the Figure 4(a), dash-dotted line shows the attack on the second power and solid line indicated the TDS attack injected to the first power area which are called ''TDS attack 1'' and ''TDS attack 2'' respectively. The dashed and dotted lines illustrate the delay estimation of TDS attack 2 and 1 respectively. This figure demonstrates that CF-TDSR is capable of detecting and tracking TDS attack accurately in real-time.

The behavior of the LFC distributed power system under attack in three scenarios was evaluated. The first scenario called ''Baseline'' runs without any modification to the communication protocol and to the controller (dotted line). The second scenario called the ''CF-TDSR-Type1'' evaluates the LFC under the attack using an adaptive communication protocol while the controller is not adaptive (dashed line). The third scenario evaluates the LFC system using the ''CF-TDSR-Type2'', i.e., both the adaptive communication protocol and adaptive controller design defenses (solid line).

Figure 4 shows that the CF-TDSR-Type2 is capable of quickly detecting the TDS attack and adapt the communication protocol and controller. Note that when CF-TDSR detects a delay larger than 0.4s, it sends an NACK to the sender, as suggested by the study of eigenvalues for the stability of the system [4]. Figures 4 (b)-(f) show the frequency deviation, the power deviation of the generator, the value position of the turbine and the tie-line power flow of the first power area, respectively. They show that the system becomes stable when using CF-TDSR-Type 1 or Type 2 and system gets unstable using baseline.

Based on the results, we conclude that if CF-TDSR detects a TDS attack on the second channel and there is no more communication channel available, the estimator turns on and

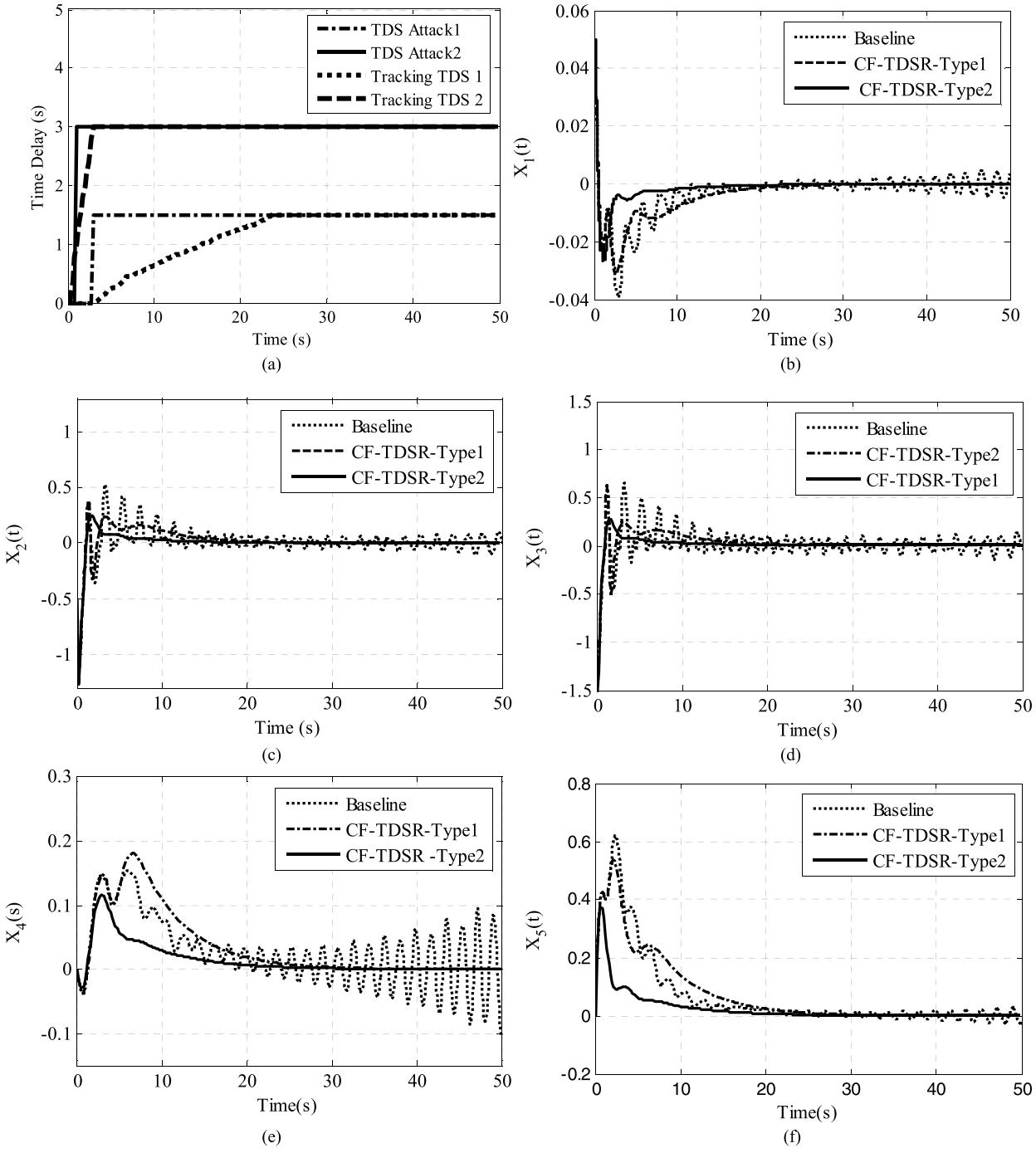

FIGURE 4. Composite TDS attack on one state of a two-area power system. Here, the results of the attack on the first power area are illustrated. It is shown that how long it takes to stabilize the system under TDS attack. (a) Time-delay attack on system (solid line is attack on third state of first power area and dashed line shows TDS attack on the third state of the second power area). (b) Frequency deviation during the attacks. (c) Power deviation of the generator during the attack. (d) Value position of the turbine during the attack. (e) Tie-line power flow and finally figures the control error.

stays alive for the entire time and guarantees the stability of the system. The results show that CF-TDSR works very well, even with strict limitations on the number of available channels, which is evidenced by converging all states to zero as expected. The results also indicate that the system become unstable under TDS attack without any defense mechanism, ''Baseline''. Furthermore, Figure 4 (b)-(f) indicated that CF-TDSR type 2 has better performance than CF-TDSR-type 1 while both of them stabilized the system fairly.

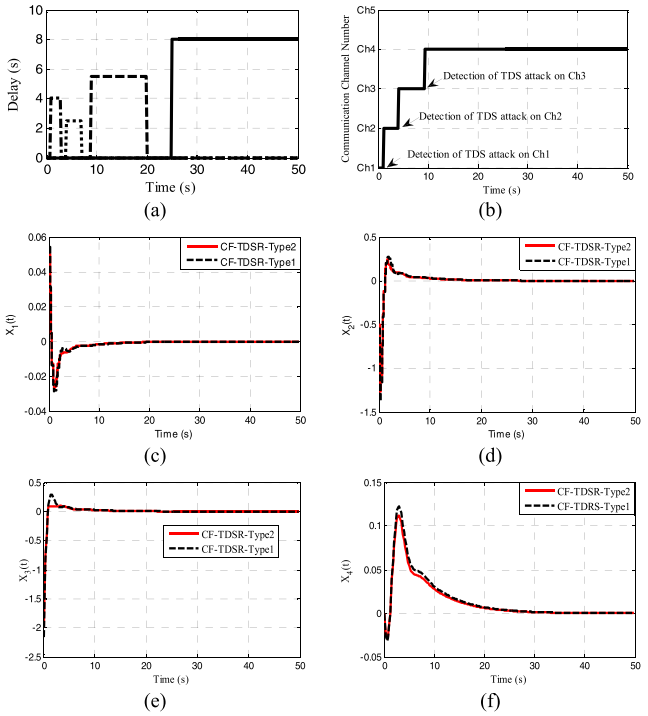

FIGURE 5. TDS attack on one power area. (a) Illustration of a sophisticated, sequential, multi-channel attack: each of the 4 bumps corresponds to a TDS attack launched on a different channel. (b) Evolution in time of CF-TDSR: the time when CF-TDSR detects each attack and requests a change of channel. The attack on channel 4 is not effective because the system has already approached the stable region. (c) The frequency deviation of the power system during the attacks. (d) The power deviation of the generator during the attacks. (e) The evolution in time of the value position of the turbine during the attacks. (f) The tie-line power flow during the attack. Figures 4(c)-(f) compare CF-TDSR (solid line) to a version where the state estimator is off (black dashed line). CF-TDSR greatly improves over a state estimator-free version.

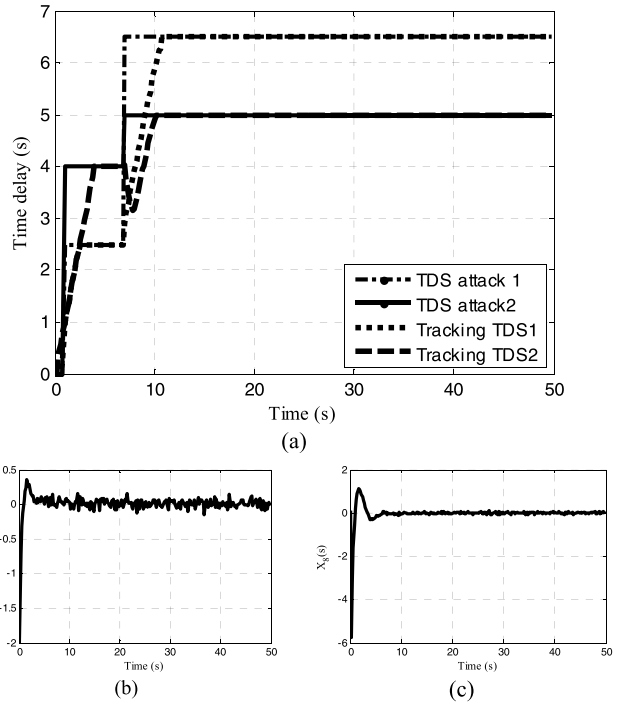

FIGURE 6. TDS attack injected at the same time on both power areas. After a period of time, the attacker increased the value of attack, as shown in (a). The TDS tracker is shown in (a). Value positions of the turbine, ΔP_{tu} for the first and the second power area are shown in (b) and (c) respectively. There is only one channel for our defense; hence, the detector tracked the attack in real time. The system experienced noise and disturbances.

B. SINGLE-PLANT TDS ATTACK

In the second case, we assume that a hacker only has access to the first power area, and can only launch TDS attacks on the specific state variable. The existence of multiple channels for allocation is assumed, but the CF-TDSR-Type2 method only needs a limited number of channels due to its adaptive controller feature of CF-TDSR protocol. It's assumed that a powerful hacker can launch multiple and sequential TDS attacks.

Figure 5 shows the results of the simulation. Figure 5(a) describes the attack that was launched: the dash-dotted line denotes a TDS attack on the first communication channel that occurs at time 1-3 seconds with a delay of 4 seconds, followed by a TDS attack on channel 2 between 3-4 seconds, with a delay of 2.5 seconds (dotted line), and then a TDS attack on the channel 3 between 9-20 seconds (dashed line) and a TDS attack on the channel 4, with a delay of 9 seconds, from time 25 seconds to 50 seconds (solid line). Figure 5(b) shows that the CF-TDSR protocol detects each attack and requests a change of channel accurately. The attack on the channel 4 is not effective because the system has already approached the stable region. The conclusion is that when the system is at optimal value (close to zero), it is more difficult for the TDS attack or other types of attacks to destabilize the system.

Figure 5(c) shows the frequency deviation, Δf^K, of the power system. Figure 5(d) shows the power deviation of the generator, Δf_g^K. Figure 5(e) shows the value position of the turbine, Δf_{tu}^K. Figure 5(f) shows Tie-line power flow, Δf_{pf}^l. These figures prove that our states remain stable and converge to zero under a TDS attack. Figures 5(c)-5(f) compared the results of a scenario where the state estimator is on and controller is adaptive (CF-TDSR-Type2, shown in solid line) to the results of a scenario where the state estimator is off (dashed line). In both cases, the time-delay detector and channel adaptation are on. The figures show that the CF-TDSR protocol is clearly superior. The results indicate that the cost function value is improved, ($\Delta J = J_{No\ Estimation} - J_{With\ Estimation} = 5.21$), when our state estimator is running which take cares of a TDS attack while the NACK signal receives by transmitter and a new channel is added to the system.

The comparison between single plant TDS attack and composite TDS attack indicated that CF-TDSR is capable of detecting and compensating the effect of TDS attack in general. It also shows that CF-TDSR-Type 2 is better than type 1 in both cases but, it's much more powerful than type1 in the case that there is a limitation with existence of redundant communication channels.

C. SIMULTANEOUSLY TDS ATTACK FOR THE NOISY SYSTEM AND LIMITED AVAILABLE CHANNEL

In the last experiment, the system behavior under the noise is studied. In order to do this, first, 20% of white Gaussian noise is added to the communication channel. Then, a TDS attack is launched on both power areas:

The attacker simultaneously launches the attack on the third state of both the first and the second power areas at time 1 second and 4 sec, with a 2-seconds delay. Then, the delay value is increased at time 7 sec to the value of 5 sec and 6.5 sec. In this experiment, the availability of a single communication channel is assumed. This assumption severely restricts the CF-TDSR's options so we only can use CF-TDSR-Type 2.

Figure 6 shows that even under such restrictions, the CF-TDSR is able to accurately detect and reduce the effects of the noise based TDS attack. Specifically, Figure 6 (a) shows how CF-TDSR detects and tracks the TDS attack in real time. Figures 6 (b) and (c) show the third states of the first and second power areas under the noise based TDS attack. They show that CF-TDSR performs very well even in the absence of additional communication channels and existence of noise.

VII. CONCLUSION

Networked control systems used in power systems share information via a variety of communication protocols, making them vulnerable to attack by hackers at any infrastructure point. In this article, different types of time delay switch attacks were the main focus. The CF-TDSR, a communication protocol that uses adaptive channel redundancy techniques, as well as a novel state estimator was developed to detect and obviate instable effects of a TDS attack. It was demonstrated that the CF-TDSR enabled the linear time-invariant control systems to remain stable. The simulation experiments show the CF-TDSR enabling the multi-area load frequency control component to quickly stabilize the system under a suite of TDS attacks.

REFERENCES

[1] K. Boroojeni, M. H. Amini, A. Nejadpak, T. Dragičević, S. S. Iyengar, and F. Blaabjerg, "A novel cloud-based platform for implementation of oblivious power routing for clusters of microgrids," *IEEE Access*, vol. 5, pp. 607–619, 2017.

[2] S. Xie, J. Yang, K. Xie, Y. Liu, and Z. He, "Low-sparsity unobservable attacks against smart grid: Attack exposure analysis and a data-driven attack scheme," *IEEE Access*, vol. 5, pp. 8183–8193, 2017.

[3] A. A. Cárdenas, S. Sastry, and S. Amin, "Safe and secure networked control systems under denial-of-service attacks," in *Proc. 12th Int. Conf. Hybrid Syst.*, San Francisco, CA, USA, 2009, pp. 31–45.

[4] P. Eder-Neuhauser, T. Zseby, and J. Fabini, "Resilience and security: A qualitative survey of urban smart grid architectures," *IEEE Access*, vol. 4, pp. 839–848, 2016.

[5] 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.

[6] A. Sargolzaei, K. Yen, and M. Abdelghani, "Time-delay switch attack on load frequency control in smart grid," in *Proc. Innov. Smart Grid Technol. Conf.*, vol. 5. Feb. 2014, pp. 1–5.

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

[8] J. Nilsson, "Real-time control systems with delays," Lund Inst. Technol., Lund, Sweden, Tech. Rep., 1998.

[9] S. Falasca, M. Gamba, and A. Bicchi, "Output-feedback dynamic control over packet-switching networks," in *Informatics in Control, Automation and Robotics*. Cham, Switzerland: Springer, 2015, pp. 177–200.

[10] M. Ergen, S. Coleri, and P. Varaiya, "QoS aware adaptive resource allocation techniques for fair scheduling in OFDMA based broadband wireless access systems," *IEEE Trans. Broadcast.*, vol. 49, no. 4, pp. 362–370, Dec. 2003.

[11] N. A. Odhah *et al.*, "Adaptive resource allocation algorithms for multi-user MIMO-OFDM systems," *Wireless Pers. Commun.*, vol. 80, no. 1, pp. 51–69, 2015.

[12] Z. Shen, J. G. Andrews, and B. L. Evans, "Adaptive resource allocation in multiuser OFDM systems with proportional rate constraints," *IEEE Trans. Wireless Commun.*, vol. 4, no. 6, pp. 2726–2737, Nov. 2005.

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

[14] 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.

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

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

[17] 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.

[18] R. Grondin, Y. Hebert, and I. Kamwa, "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.

[19] H. 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.

[20] J. Quanyuan, Z. Zhenyu, and C. Yijia, "Wide-area TCSC controller design in consideration of feedback signals' time delays," in *Proc. IEEE Power Eng. Soc. Gen. Meet.*, vol. 2. Jun. 2005, pp. 1676–1680.

[21] 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.*, Jun. 2005, pp. 4357–4362.

[22] R. Majumder, B. Pal, and B. Chaudhuri, "Wide area measurement based stabilizing control of power system considering signal transmission delay," in *Proc. IEEE Power Eng. Soc. Gen. Meet.*, Jun. 2005, pp. 1447–1450.

[23] 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.

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

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

[26] 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.

[27] L. Chunmao and X. Jian, "Adaptive delay estimation and control of networked control systems," in *Proc. Int. Symp. Commun. Inf. Technol.*, Oct. 2006, pp. 707–710.

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

[29] 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.

[30] 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.

[31] H. A. Shayanfar, A. Jalili, and H. Shayeghi, "Load frequency control strategies: A state-of-the-art survey for the researcher," *Energy Convers. Manage.*, vol. 50, no. 2, pp. 344–353, 2009.
[32] 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.
[33] H. Bevrani, *Robust Power System Frequency Control*. New York, NY, USA: Springer, 2009.

ARMAN SARGOLZAEI received the M.Sc. degree in electrical and computer engineering from Florida International University, Miami, FL, USA, in 2012, and the Ph.D. degree in electrical engineering from Florida International University, in 2015. He is currently an Assistant Professor with the department of electrical engineering, Florida Polytechnic University. He has authored over 50 journal and conference papers in his field of interest. His research interests include security of networked control systems, robotics, nonlinear control systems, and power systems. He also is part of Editorial Board and Reviewer of a few journal papers, such as *Asian Journal of Control*, the IEEE TRANSACTIONS ON SMART GRID, the IEEE TRANSACTIONS ON CYBERNETICS and many others.

KANG K. YEN received the Ph.D. degree from Vanderbilt University in 1985. He is currently a Full Professor, Professional Engineer, and a Graduate Coordinator with the Electrical and Computer Engineering Department, Florida International University. He has authored over 150 journal and conference papers. His research interests include system modeling and simulation, control theory, parallel processing, microprocessor, and AI applications.

MOHAMED N. ABDELGHANI received the Ph.D. degree in mathematics and statistics from the University of Alberta in 2016, the master's degree in electrical and computer engineering from Southern Illinoise University, and the Ph.D. degree in neuroscience from the University of Toronto. His research interests include stochastic control, sensory motor control, and neural information processing.

SAMAN SARGOLZAEI received B.Sc. and M.Sc. degree in electrical engineering in 2006 and 2009, the second M.Sc. degree in electrical engineering from the Universty of Miami, Miami, USA, in 2012 and the Ph.D. degree in electrical engineering from Florida International University, Miami, USA, in 2015. He is currently involved in NMDAR-Mediated Dysfunction in a Pediatric Traumatic Brain Injury Model. His expertise is in applying machine learning and artificial intelligence to the field of medicine and biology for a more efficient health care, following his vision to live in a world without disease and disability. His research on comprehensive map of brain neural connections carried significant practical implications in better understanding the pathways of neurological disorders.

BOGDAN CARBUNAR received the Ph.D. degree in computer science from Purdue University. He is currently an Assistant Professor with SCIS, Florida International University. He held various researcher positions with the Applied Research Center, Motorola. His research interests include distributed systems, security and applied cryptography.