Scientific
Research
Publishing

A Novel Technique for Detection of Time Delay Switch Attack on Load Frequency Control

Arman Sargolzaei[1], Kang K. Yen[1], Mohamed N. Abdelghani[2], Abolfazl Mehbodniya[3], Saman Sargolzaei[4]

[1]Department of Electrical and Computer Engineering, Florida International University, Miami, FL, USA
[2]Department of Mathematics and Statistics, University of Alberta, Edmonton, Canada
[3]Graduate School of Engineering-Sendai, Tohoku University, Sendai, Japan
[4]Department of Electrical and Computer Engineering, Wentworth Institute of Technology, Boston, MA, USA
Email: arman.sargolzaei@rancsgroup.com

Abstract

In this paper, we focus on the estimation of time delays caused by adversaries in the sensing loop (SL). Based on the literature review, time delay switch (TDS) attacks could make any control system, in particular a power control system, unstable. Therefore, future smart grids will have to use advanced methods to provide better situational awareness of power grid states keeping smart grids reliable and safe from TDS attacks. Here, we introduce a simple method for preventing time delay switch attack on networked control systems. The method relies on an estimator that will estimate and track time delays introduced by an adversary. Knowing the maximum tolerable time delay of the plant's optimal controller for which the plant remains stable, a time-delay detector issues an alarm signal when the estimated time delay is larger than the minimum one and directs the system to alarm state. In an alarm state, the plant operates under the control of an emergency controller that is local to the plant and remains in this mode until the networked control system state is restored. This method is an inexpensive and simple way to guarantee that an industrial control system remains stable and secure.

Keywords

Time Delay Switch Attack, Load Frequency Control, Detection and Estimation, Emergency Controller

1. Introduction

Modern power grids rely on telecommunication technologies for control and monitoring, in a way to improve efficiency and reliability distribution. However, their reliance on computers and multi-purpose networks makes them vulnerable to cyber-attacks [1]-[3]. Recently, the investigation of attack methods on industrial control systems and their countermeasures have been the focus of many academic, industries, and governments. Here, we will investigate one type of attacks on a power control system recently proposed by Sargolzaei *et al.* [4]-[6] that is time delay switch attack and we provide a simple detection/estimation technique for time delays caused by an adversary. State estimation is one of the pivotal features of future power systems [7]. According to [8], improving the resiliency and reliability of smart distribution networks could be obtained via deploying renewable resources and demand side management programs. As it has been mentioned in [9], demand response can ameliorate the load curve by motivating smart customers utilizing smart communication infrastructure and smart meters.

The controller design for systems with time delay is one of the interests of many researchers [10]-[12] but they have not studied that time delay can be injected to the system as an attack. Time delays injected by a hacker in a control system would, in general, destabilize the system or cause inefficiency in performance of the system. This is a new attack in the context of power systems (e.g., load frequency control (LFC)) on networked control systems (NCS) [13] and is named time-delay-switch attack or TDS for short [4]. To avoid possible damage of TDS attacks, systems and controllers must be redesigned in a way to detect and correct for variable time delays.

Time delays exist in power systems, in the sensing and control loops. The traditional controllers of power systems are designed based on current information being available and ignoring time delays even if they present. However, power grids technologies are continuously being improved by introducing new telecommunication technologies for monitoring to improve 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 which are used for stability analysis of power systems can also be used for designing more robust controllers. Nevertheless, time delays are present in PMUs measurements as a result of natural transmission lines [14].

Several studies have considered the problem of stability of power systems with time delays [10] [11]. The impact of time delays on the power system controllers was discussed in [15]-[19]. In [20], authors studied the effects of delays on the small signal stability of power systems. In [15] and [16], methods to eliminate oscillations that resulted from time-delayed feedback control were proposed. Authors in [21] presented a wide-area control system for damping generator oscillations. Using phasor measurements, but with delays, a controller was proposed in [14] and small signal stability of the power system was considered. A feedback controller designed for power systems with delayed states was proposed in [22]. 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 delay can be found in [2] [3] [10]-[12] [23]-[25] and the references therein. However, most of these studies considered either the construction of controllers that were robust to time delays or controllers that used offline estimate of time delays. As far as we know, there are no control methods that perform online estimation of dynamic time delays and real time control of power systems. Furthermore, few studies [26] [27] considered control of power systems with time delays introduced by adversary.

In this paper, we will describe a simple yet effective method to address a TDS attack on the observed states of a controlled system. Our method utilizes a time delay estimator, a communication protocol to alarm for time delay switch attack, a buffer to store the history of controller commands and an optimal controller to stabilize or track a reference signal and a local to the plant emergency controller to stabilize the plant if large time delays are detected. For now, we will only deal with LTI systems in state feedback.

2. Method

All control methods developed in the past compensate for time delays either rely on controller robust to a maximum time delay, off-line estimates of time delays or approximation of time delayed signals [26] [27]. Here, we develop an alternative time delay estimator which is simpler and will help with systems under time delay attack. In this paper, we propose a general method for control of systems under TDS attack. We have developed this method for continuous linear time-invariant systems. We have implemented our models and control strategies in MATLAB to demonstrate the performance with simulation.

The proposed method is shown in **Figure 1**. Its basic elements are: plant model, time delay detector, emergency controller and controller. The controller can either be a PID controller or an optimal feedback controller. The emergency controller's job is to stabilize the system in case of an attack on the communication lines of the distant controller. The time delay detector estimates the time delay in the communication channel from telemetered data. If the delay is larger than a maximum allowed time delay it sends alarm signals to the controller and emergency controller. If an alarm signal is received by the emergency controller it will begin to operate in a way to stabilize the plant to a desired state while the distant controller stops to operate until the delay is corrected.

Suppose the system we are dealing with is linear time invariant (LTI) or can be approximated in a region of interest by a LTI system,

$$\dot{x}(t) = Ax(t) + Bu(t),$$ (1)

where x and u are state and control vectors, respectively. Matrices A and B are constant matrices with suitable dimensions.

Then, the solution is given by

$$x(t) = e^{At}x_0 + \int_0^t e^{A(t-s)} Bu(s) \, ds$$ (2)

with time delay τ, either a time-delay switch attack or a natural delay, the solution of Equation (2) becomes

$$x(t-\tau) = e^{A(t-\tau)}x_0 + \int_0^{t-\tau} e^{A(t-\tau-s)} Bu(s) \, ds \, .$$ (3)

Let us write the solution $x(t)$ at the time t in terms of the solution with the time delay τ; we have

$$x(t) = e^{At}x_0 + e^{A\tau}\int_0^{t-\tau} e^{A(t-s)}e^{-A\tau} Bu(s) \, ds + \int_{t-\tau}^t e^{A(t-s)} Bu(s) \, ds$$
$$= e^{At}x_0 + e^{A\tau}\left[x(t-\tau) - e^{A(t-\tau)}x_0\right] + \int_{t-\tau}^t e^{A(t-s)} Bu(s) \, ds,$$ (4)

In general, the time delay τ is an unknown variable. Let's assume that τ is slowly varying, compared to the changes in u and x, and $\hat{\tau}$ is our estimate of the time delay τ. Then, $\varepsilon = \hat{\tau} - \tau$ is the estimation error in the time delay. The predicted state $\hat{x}(t)$ of the system based on the estimate of time delay $\hat{\tau}$ is given by

$$\hat{x}(t) = e^{At}x_0 + e^{A\hat{\tau}}\left[\hat{x}(t-\hat{\tau}) - e^{A(t-\hat{\tau})}x_0\right] + \int_{t-\hat{\tau}}^t e^{A(t-s)} Bu(s) \, ds$$ (5)

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

It should be noted that, $x(t-\tau)$ is what we actually measures and deliver to the plant model. So, at every instance of time, the 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's essential that the plant model estimates state $x(t)$ accurately. Because of the delay, an accurate enough estimation of $x(t)$ requires a good estimate of the delay τ. We will show how to estimate the delay τ.
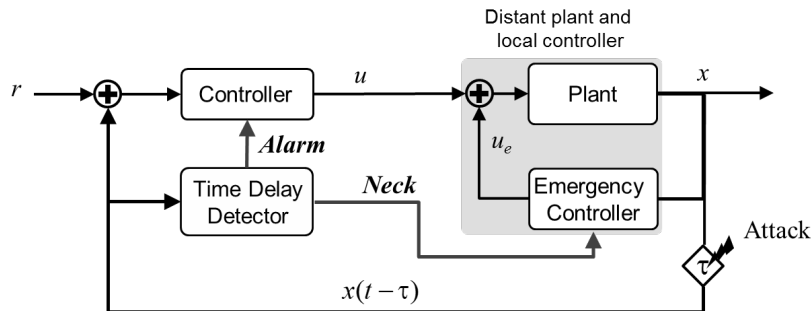

Figure 1. Block diagram of the proposed control system.

The estimation error in states can be described by $e_m(t) = x(t) - \hat{x}(t)$ and with delay it is given by

$$e_m(t; \tau, \hat{\tau}) = x(t - \tau) - \hat{x}(t - \hat{\tau}). \tag{6}$$

Then the idea is to estimate $\hat{\tau}$ overtime as fast as possible to minimize the error $e_m(t; \tau, \hat{\tau})$. Using the gradient descent method, we set

$$\frac{d\hat{\tau}}{dt} = -\eta \frac{\partial v}{\partial \hat{\tau}}, \tag{7}$$

where η is the learning parameter and select $v = \frac{1}{2} e_m^2$. With some manipulation, we have

$$
\begin{aligned}
\frac{d\hat{\tau}}{dt} &= -\eta e_m \frac{\partial e_m}{\partial \hat{\tau}} = -\eta e_m \frac{\partial \left[x(t-\tau) - \hat{x}(t-\hat{\tau}) \right]}{\partial \hat{\tau}} \\
&= \eta e_m \frac{\partial \hat{x}(t-\hat{\tau})}{\partial \hat{\tau}} = \eta e_m \frac{\partial}{\partial \hat{\tau}} \left[e^{A(t-\hat{\tau})} x_0 + \int_0^{t-\hat{\tau}} e^{A(t-\hat{\tau}-s)} Bu(s) ds \right]. \\
&= \eta e_m \frac{\partial}{\partial \hat{\tau}} \left[\int_0^{t-\hat{\tau}} e^{A(t-\hat{\tau}-s)} Bu(s) ds \right] - \eta e_m A e^{A(t-\hat{\tau})} x_0 \\
&= -\eta e_m \left[Bu(t-\hat{\tau}) - e^{A(t-\hat{\tau})} Bu(0) - A e^{A(t-\hat{\tau})} x_0 \right]
\end{aligned}
\tag{8}
$$

Assuming that, $u(0) = 0$, which is reasonable for initial time, we arrive at

$$\frac{d\hat{\tau}}{dt} = -\eta e_m Bu(t-\hat{\tau}) - A e^{A(t-\hat{\tau})} x_0, \qquad 0 \le \hat{\tau} \le t \tag{9}$$

Equation (9) is the one we will use to estimate the time delay τ. However, there are practical issues that we need to consider. Computing machines have finite memory and temporal resolution. Therefore, we are unable to implement Equation (9) without discrete approximation and boundedness assumptions. To guarantee stability of calculations and limit our memory usage we have to add the following condition, $\tau < \tau_{max}$. This condition will allow us to construct a finite buffer to store the history of $u(t)$ from t to $t - \tau_{max}$.

After designing the time delay estimator, we turn our attention to the controller and emergency controller. The controller can either be a PID controller or an optimal controller depending on the requirements of the application. Equation (10) is the PID controller and Equation (11) is the optimal controller,

$$u(t) = K_P e(t) + K_D \frac{de}{dt}(t) + K_I \int_0^t e(s) ds, \tag{10}$$

$$u(t) = K e(t). \tag{11}$$

where the error is $e(t) = r(t) - x(t)$. Either controller, *i.e.*, the PID or the optimal controller, can be designed in a way to be robust to some maximum time-delay τ_{stable}. The emergency controller sits close to the plant and operates only in case of emergency, for example, an attack on the communication line between the plant and controller. The emergency controller could either be a PID controller or optimal controller with the goal to stabilize the system to a particular reference trajectory r_E.

Suppose there is a time delay attack on the system with delay τ; the time delay estimator will estimate the delay $\hat{\tau}$. The cyber-attack detector will use the time delay estimate to perform the following function

$$D = \begin{cases} 1 & \hat{\tau} > c\tau_{stable} \\ 0 & \text{otherwise} \end{cases}, \tag{12}$$

where c is a constant between 0 and 1. In case $D = 1$ an alarm signal is sent to the controller to shut it down and a negative acknowledgement is sent to the emergency controller to stabilize the plant. The control strategy is shown in **Figure 1**.

We have implemented this method in MATLAB and verified its performance using the load frequency control (LFC) of a two-area distributed power system. In the next section we present and discuss the simulation results.

3. Result

We focus on the LFC system where the controller's function is to regulate the states of a networked power plant. The multi interconnect LFC dynamic system description can be found in [4]. Here we focus on two-area power system with the attack model as

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

(13)

The optimal feedback controller is given by

$$U(t) = -K\hat{X}(t)$$

(14)

and the new state after the attack can be modeled by

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

(15)

where $\tau = \left[t_{d1}, t_{d2}, \cdots, t_{dN}\right]^{\mathrm{T}}$ are different/random time-delays and are positive values. When $t_{d1}, t_{d2}, \cdots, t_{dN}$ are all zero, the system is in its normal operation. An adversary can get access to the communication link and inject a delay attack on the line to direct the system to abnormal operations.

In (13), $X(t) = \left[x_1(t) \quad x_2(t)\right]^{\mathrm{T}}$ denotes the states in the first and second power areas. Then the state vector in the ith power area is defined as

$$x_i(t) = \left[\Delta f^i(t) \quad \Delta P_g^i(t) \quad \Delta P_{tu}^i(t) \quad \Delta P_{pf}^i(t) \quad \Lambda^i(t)\right]^{\mathrm{T}} \qquad i = 1, 2,$$

(16)

where $\Delta f^i(t)$, $\Delta P_g^i(t)$, $\Delta P_{tu}^i(t)$, $\Delta P_{pf}^i(t)$ and $\Lambda^i(t)$ are frequency deviation, power deviation of the generator, position value of the turbine, tie-line power flow, and control error on the ith power area, respectively [19]. The control error of the ith power area is expressed as

$$\Lambda^i(t) = \int_0^t \beta_i \Delta f^i(s)\,\mathrm{d}s,$$

(17)

where β_i denotes the frequency bias factor.

In the dynamic model of the two-area LFC (13):

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix},$$

(18)

$$B = \mathrm{diag}\left\{\left[B_1^{\mathrm{T}} \quad B_2^{\mathrm{T}}\right]^{\mathrm{T}}\right\},$$

(19)

$$D = \mathrm{diag}\left\{\left[D_1^{\mathrm{T}} \quad D_2^{\mathrm{T}}\right]^{\mathrm{T}}\right\},$$

(20)

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

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

(21)

$$B_i = \begin{bmatrix} 0 & 0 & \dfrac{1}{T_{g\,i}} & 0 & 0 \end{bmatrix}^T \tag{22}$$

$$A_{ij} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -2\pi T_{ij} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{23}$$

and

$$D_i = \begin{bmatrix} -\dfrac{1}{J_i} & 0 & 0 & 0 & 0 \end{bmatrix}^T \tag{24}$$

where i and j can only be values one and two, 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 ith power area and T_{ij} is the stiffness constant between the ith and the jth power areas, respectively.

The analysis starts with the design of an optimal controller for the LFC in the normal operation (*i.e.*, with no attack). Consider the system model described by (13) with the performance index described by

$$J = \frac{1}{2} \int_0^{t_f} \left\{ X^T(t)QX(t) + U^T(t)RU(t) \right\} dt, \tag{25}$$

where matrix $Q \in R^{n \times n}$ is positive semi-definite and $R \in R^{m \times m}$ is positive definite. Then, the optimal control problem is to obtain optimal control $U^*(t)$ that minimizes the performance index (25), subject to the dynamic of the system with no time-delay in its states.

Simulation studies have been conducted to evaluate the effects of TDS attacks on the dynamics of the system and detect TDS attacks to direct the controller to emergency state. By solving the Riccati matrix equation we obtain the close loop control law in the form of state feedback. For the simulations we have used discrete linear-quadratic regulator design from continuous cost function called "lqrd" function in MATLAB 2013a. **Table 1** shows parameter values used in this process. We also set both ΔP_l^1 and ΔP_l^2 to zero.

In our simulation, the total simulation time is 50 second and the sampling time is 0.01 s as its common in industrial applications. To show accuracy of our proposed TDS attack detector/tracker, we didn't send negative acknowledgment to the local controller for the first simulation to only track the injected time delay to the system. The simulation has been done for three different scenarios: 1) single TDS attack on one power area, 2) Simultaneous TDS attack on both power areas, 3) Complex varied TDS attack on both power areas.

1) Single TDS attack to one power area: Here, we considered that adversary attacks the third state of the first power area at time of 2 second for a delay value of 3 seconds and the time delay is increased to 4.5 seconds at time of 7 seconds. **Figure 2** shows that the detector accurately tracked and monitored the TDS attack or any

Table 1. 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}	0.18 s
R	100 I	Q_f	0
Q	100 I	t_f	∞
β_1	21.5	β_2	21

natural delay on the system.

2) Simultaneous TDS attack to both power areas: In this scenario, we attack the third state of both power areas. TDS attacks 1 and 2 have been injected to the first and the second power areas respectfully. TDS attack 1 is started at time 2 seconds for value 3 seconds and increased at time 8 seconds to the value of 4.5 seconds. Also TDS attack 2 is started simultaneously with TDS attack 1 for the value of 1.5 seconds and increased to the value of 6 seconds. **Figure 3** shows the result.

3) Complex varied TDS attack to both power areas: In the last scenario we injected the TDS attack at different time with different time-delay values. We assume that an adversary injects TDS attack to feedback lines of both power areas. In our simulation, an attacker starts TDS attack to the second power area (third state) at time 1 second for $t_{d3} = 5\,\text{s}$ and then increases it to $t_{d3} = 10\,\text{s}$ at 20 second. Furthermore, adversary starts to attack the first power area (third state), at 1 second with $t_{d8} = 3\,\text{s}$ and increased it to $t_{d8} = 4.5\,\text{s}$ at 30 second. **Figure 4** and **Figure 5** show TDS attack tracking real time. **Figure 4** shows TDS attack on the third state of the first power area and **Figure 5** shows the attack on the same state of the second power area.

For the second part of our simulation we enabled the emergency controller to show the effect of our proposed technique for overcoming the TDS attack. We assume that an adversary injects TDS attack to the feedback lines of both power areas. In the simulation, a TDS attack was applied to the second power area (the third state) at time of 1 second for $t_{d3} = 5\,\text{s}$ and then increases it to $t_{d3} = 10\,\text{s}$ at 20 second. Furthermore, adversary starts to attack the first power area (the third state), at 1 second with $t_{d8} = 3\,\text{s}$ and increased it to $t_{d8} = 4.5\,\text{s}$ at 30 second. We also set the $\tau_{\text{stable}} = 0.4\,\text{s}$ based on stability analysis of LFC system in [4]. We send the negative acknowledgment to emergency controller in the case that detected value of time-delay is more than the maximum allowed time-delay. **Figure 6** and **Figure 7** show the third state of the first and the second power areas
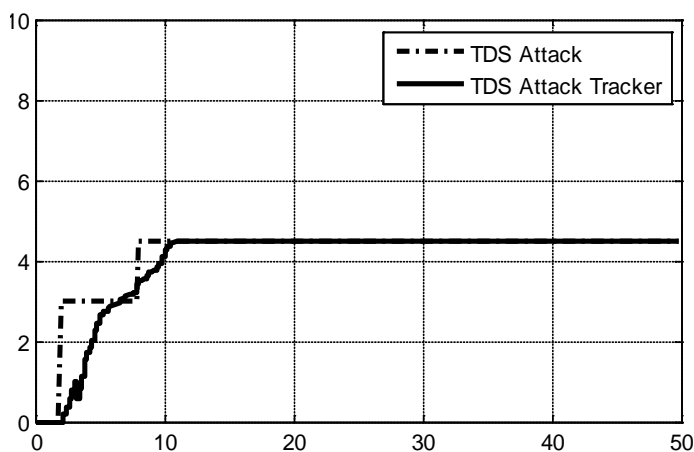

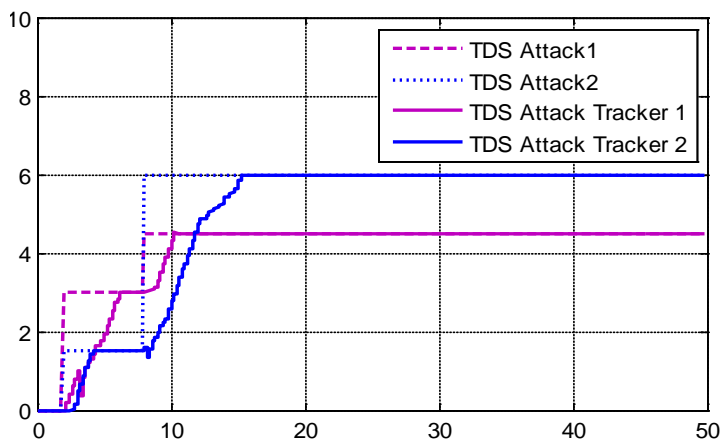**Figure 2.** TDS attack detection and tracking for third state of first power area.

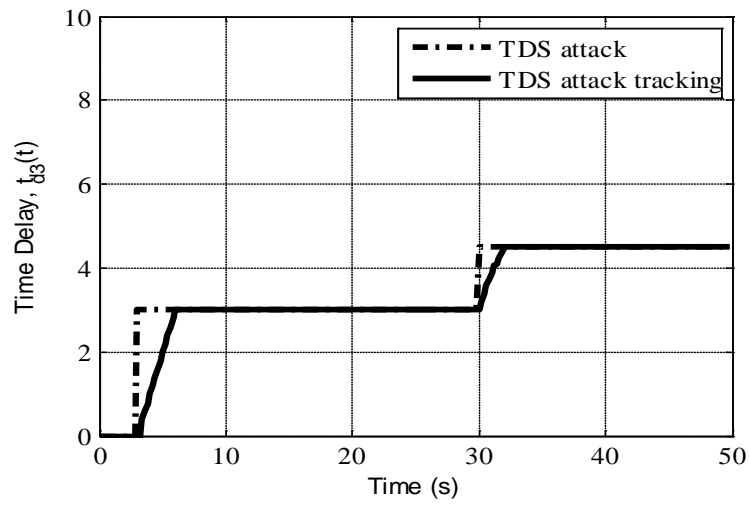**Figure 3.** TDS attack detection and tracking for simultaneous TDS attack on both power areas.

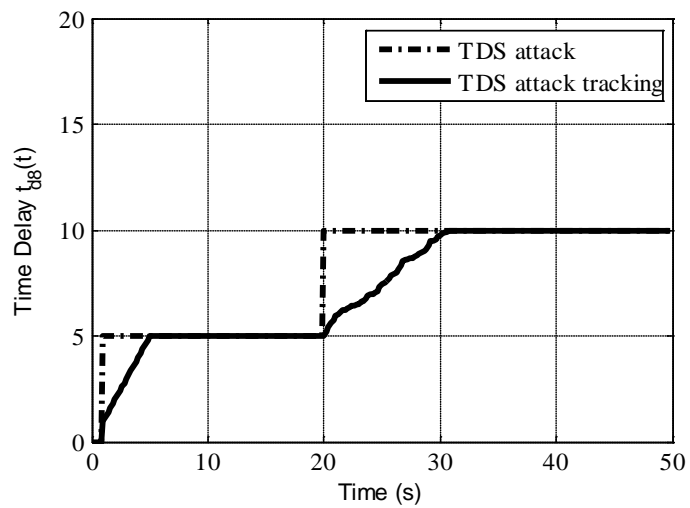**Figure 4.** TDS attack detection and tracking for third state of first power area.

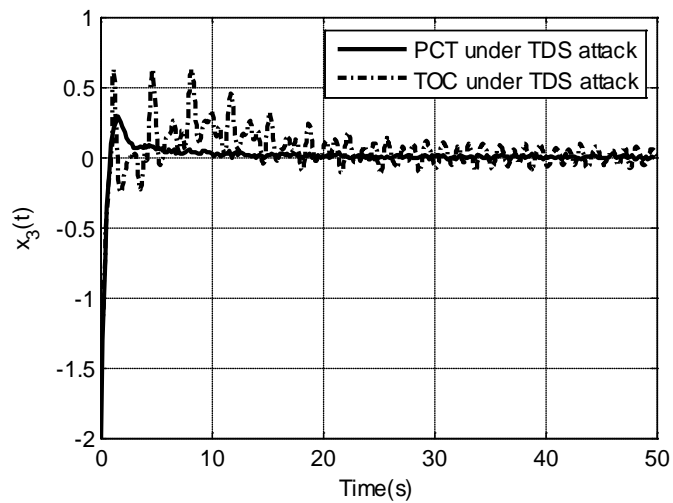**Figure 5.** TDS attack detection and tracking for third state of second power area.

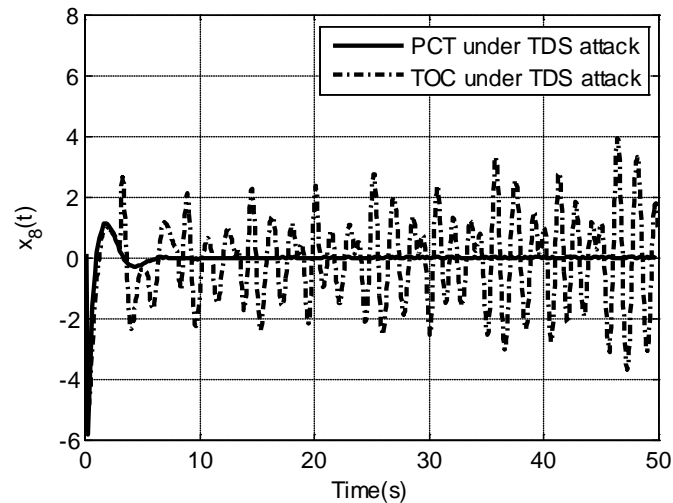**Figure 6.** Value position of the turbine system under TDS attack for the first power-area control system.

Figure 7. Value position of the turbine system under TDS attack for the second power-area control system.

under attack with traditional optimal controller (TOC) and the proposed control technique (PCT) respectively. As it's clear on the result, the simulated attack makes the system unstable. With the proposed technique, we could overcome TDS attack on the simulated system.

4. Conclusion

In summary, we have demonstrated a simple method for estimating and detecting time delay switch attack on a networked control system. The method relies on a time delay estimator that estimates and tracks time-delays introduced by an adversary. With knowledge of the maximum time delay of the control system, for which the plant remains stable and secure, the time-delay detector compares the estimated time delay to the maximum allowed time delay and issues an alarm signal when the estimated time delay is larger than this value. It also directs the system to an alarm state. In an alarm state, the plant is under the control of the emergency controller, which is local to the plant. The plant remains in this mode until the networked control system state is restored and time-delay switch is eliminated. We think that this method is simple and an inexpensive way to assure that an industrial control system remains stable and secure.

Acknowledgements

References

[1] Ericsson, G.N. (2010) Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure. *IEEE Transactions on Power Delivery*, **25**, 1501-1507. http://dx.doi.org/10.1109/TPWRD.2010.2046654

[2] Zhang, C.-K., Jiang, L., Wu, Q.H., He, Y. and Wu, M. (2013) Delay-Dependent Robust Load Frequency Control for Time Delay Power Systems. *IEEE Transactions on Power Systems*, **28**, 2192-2201.

[3] Yuan Y.L., Li Z.Y. and Ren, K. (2011) Modeling Load Redistribution Attacks in Power Systems. *IEEE Transactions on Smart Grid*, **2**, 382-390.

[4] Sargolzaei, A., Yen, K. and Abdelghani, M.N. (2014) Time-Delay Switch Attack on Load Frequency Control in Smart Grid. *Journal of Advanced Communication Technologies*, **5**, 55-64.

[5] Sargolzaei, A., Yen, K. and Abdelghani, M.N. (2014) Delayed Inputs Attack on Load Frequency Control in Smart Grid. *Innovative Smart Grid Technologies Conference* (*ISGT*), 2014 *IEEE PES*, Washington DC, 19-22 February 2014, 1-5. http://dx.doi.org/10.1109/isgt.2014.6816508

[6] Sargolzaei, A., Yen, K.K. and Abdelghani, M.N. (2014) Control of Nonlinear Heartbeat Models under Time-Delay-

Switched Feedback Using Emotional Learning Control. *International Journal on Recent Trends in Engineering & Technology*, **10**, 2.

[7] Amini, M.H., Sarwat, A.I., Iyengar, S.S. and Guvenc, I. (2014) Determination of the Minimum-Variance Unbiased Estimator for DC Power-Flow Estimation. 40*th IEEE Industrial Electronics Conference* (*IECON* 2014), Dallas, 29 October-1 November 2014, 114-118. http://dx.doi.org/10.1109/IECON.2014.7048486

[8] Amini, M.H., Nabi, B. and Haghifam, M.-R. (2013) Load Management Using Multi-Agent Systems in Smart Distribution Network. *IEEE PES General Meeting* 2013, Vancouver, 21-25 July 2013, 1-5. http://dx.doi.org/10.1109/pesmg.2013.6672180

[9] Kamyab, F., Amini, M. H., Sheykhha, S., Hasanpour, M. and Jalali, M.M. (2015) Demand Response Program in Smart Grid Using Supply Function Bidding Mechanism. *IEEE Transactions on Smart Grid*, 25 May 2015, 1949-3053. http://dx.doi.org/10.1109/TSG.2015.2430364

[10] Li, Y., Tong, S.C. and Li, Y.M. (2012) Observer-Based Adaptive Fuzzy Backstepping Control for Strict-Feedback Stochastic Nonlinear Systems with Time Delays. *International Journal of Innovative Computing*, *Information and Control*, **8**, 8103-8114.

[11] Benzaouia, A., Ouladsine, M., Naamane, A. and Ananou, B. (2012) Fault Detection for Uncertain Delayed Switching Discrete-Time Systems. *International Journal of Innovative Computing*, *Information and Control*, **8**, 8049-8062.

[12] Sargolzaei, A., Yen, K., Noei, S. and Ramezanpour, H. (2013) Assessment of He's Homotopy Perturbation Method for Optimal Control of Linear Time-Delay Systems. *Applied Mathematical Sciences*, **7**, 349-361.

[13] Benéıtez-Péerez, H., Benéıtez-Péerez, A. and Ortega-Arjona, J. (2012) Networked Control Systems Design Considering Scheduling Restrictions and Local Faults. *International Journal of Innovative Computing*, *Information and Control*, **8**, 8515-8526.

[14] Dotta, D., Silva, A.S. and Decker, I.C. (2009) Wide-Area Measurements-Based Two-Level Control Design Considering Signal Transmission Delay. *IEEE Transactions on Power Systems*, **24**, 208-216. http://dx.doi.org/10.1109/TPWRS.2008.2004733

[15] Kamwa, I., Grondin, R. and Hebert, Y. (2001) Wide-Area Measurement Based Stabilizing Control of Large Power Systems—A Decentralized/Hierarchical Approach. *IEEE Transactions on Power Systems*, **16**, 136-153. http://dx.doi.org/10.1109/59.910791

[16] Wu, H.X., Tsakalis, K.S. and Heydt, G.T. (2004) Evaluation of Time Delay Effects to Wide-Area Power System Stabilizer Design. *IEEE Transactions on Power Systems*, **19**, 1935-1941. http://dx.doi.org/10.1109/TPWRS.2004.836272

[17] Jiang, Q., Zou, Z. and Cao, Y. (2005) Wide-Area TCSC Controller Design in Consideration of Feedback Signals' Time Delays. *IEEE Power Engineering Society General Meeting*, **2**, 1676-1680.

[18] Saad, M.S., Hassouneh, M.A., Abed, E.H. and Edris, A.A. (2005) Delaying Instability and Voltage Collapse in Power Systems Using SVCs with Washout filter-Aided Feedback. *American Control Conference*, **6**, 4357-4362. http://dx.doi.org/10.1109/acc.2005.1470665

[19] Chaudhuri, B., Majumder, R. and Pal, B. (2005) Wide-Area Measurement Based Stabilizing Control of Power System Considering Signal Transmission Delay. *IEEE Power Engineering Society General Meeting*, **2**, 1447-1450. http://dx.doi.org/10.1109/pes.2005.1489106

[20] Milano, F. and Anghel, M. (2012) Impact of Time Delays on Power System Stability. *IEEE Transactions on Circuits and Systems I*: *Regular Papers*, **59**, 889-900. http://dx.doi.org/10.1109/TCSI.2011.2169744

[21] Ray, S. and Venayagamoorthy, G.K. (2008) Real-Time Implementation of a Measurement-Based Adaptive Wide-Area Control System Considering Communication Delays. *IET Generation*, *Transmission & Distribution*, **2**, 62-70. http://dx.doi.org/10.1049/iet-gtd:20070027

[22] Alrifai, M.T., Zribi, M., Rayan, M. and Mahmoud, M.S. (2013) On the Control of Time Delay Power Systems. *International Journal of Innovative Computing*, *Information and Control*, **9**, 769-792.

[23] Yang, Q.Y., An, D. and Yu, W. (2013) On Time Desynchronization Attack against IEEE 1588 Protocol in Power Grid Systems. 2013 *IEEE Energytech*, Cleveland, 21-23 May 2013, 1-5.

[24] Schenato, L. (2008) Optimal Estimation in Networked Control Systems Subject to Random Delay and Packet Drop. *IEEE Transactions on Automatic Control*, **53**, 1311-1317. http://dx.doi.org/10.1109/TAC.2008.921012

[25] Mahmoud, M.S. (2000) Robust Control and Filtering for Time-Delay Systems. Marcel Dekker Inc., New York.

[26] Tan, Y.H. (2004) Time-Varying Time-Delay Estimation for Nonlinear Systems Using Neural Networks. *International Journal of Applied Mathematics and Computer Science*, **14**, 63-68.

[27] Li, C.M. and Xiao, J. (2006) Adaptive Delay Estimation and Control of Networked Control Systems. *International Symposium on Communications and Information Technologies*, 2006, *ISCIT*'06, Bangkok, 18-20 October 2006, 707-710. http://dx.doi.org/10.1109/iscit.2006.339832