electronics

MDPI

Article

A Secure Control Design for Networked Control Systems with Linear Dynamics under a Time-Delay Switch Attack

Mauro Victorio [1,†], Arman Sargolzaei [2,*,†] and Mohammad Reza Khalghani [1,†]

[1] Department of Electrical and Computer Engineering, Florida Polytechnic University, Lakeland, FL 33805, USA; mvictorio@floridapoly.edu (M.V.); Khalghani@ieee.org (M.R.K.)
[2] Mechanical Engineering Department, Tennessee Technological University, Cookeville, TN 38505, USA
* Correspondence: a.sargolzaei@gmail.com
† These authors contributed equally to this work.

Abstract: Networked control systems (NCSs) are designed to control and monitor large-scale and complex systems remotely. The communication connectivity in an NCS allows agents to quickly communicate with each other to respond to abrupt changes in the system quickly, thus reducing complexity and increasing efficiency. Despite all these advantages, NCSs are vulnerable to cyberattacks. Injecting cyberattacks, such as a time-delay switch (TDS) attack, into communication channels has the potential to make NCSs inefficient or even unstable. This paper presents a Lyapunov-based approach to detecting and estimating TDS attacks in real time. A secure control strategy is designed to mitigate the effects of TDS attacks in real time. The stability of the secure control system is investigated using the Lyapunov theory. The proposed TDS attack estimator's performance and secure control strategy are evaluated in simulations and a hardware-in-the-loop environment.

Keywords: time-delay switch attack; networked control systems; secure control design; Lyapunov theory; attack estimation; hardware-in-the-loop testing

Citation: Victorio, M.; Sargolzaei, A.; Khalghani, M.R. A Secure Control Design for Networked Control Systems with Linear Dynamics under a Time-Delay Switch Attack. *Electronics* **2021**, *10*, 322. https://doi.org/10.3390/electronics10030322

Academic Editor: Qusay H. Mahmoud
Received: 28 December 2020
Accepted: 25 January 2021
Published: 30 January 2021

1. Introduction

A networked control system (NCS) is a type of control system in which the control and feedback data packets are exchanged through communication channels between agents and the controller. NCS systems are used to enhance the efficiency and reliability of the control systems [1–4]. The simplicity and efficiency of NCSs for constructing networks among multi-agent systems have received significant attention over the past years. Although leveraging communication channels in an NCS can control and supervise the system more efficiently and reliably, NCSs are prone to cyber disruptions—either inherent or intentional ones, such as cyberattacks. The most known cyberattacks are denial of service (DoS), which disables access to the system information or a service [5], false data injection (FDI), which intentionally manipulates the exchange of data [6], replay attack, which maliciously repeats valid data transmissions [7], and a newly found attack, the time-delay switch (TDS) [3]. The number and intensity of these cyber manipulations have grown in recent years. One of these cyber attacks was the 2015 Ukraine Blackout event, in which about 225,000 customers lost their electricity for several hours. This cyber incident was a successful FDI on an actual power grid [8]. The 2019 Venezuela blackout resulted from a cyberattack on energy supplies in eighteen states that affected two-thirds of the country [9,10]. These cyber disruptions determine the criticality of studying cyber attacks on NCSs, like power grids.

A TDS attack is made by inserting time delays into communication channels of NCSs [11]. Since NCSs are time-sensitive and require updated measurement signals, a TDS can be highly destructive [11,12]. Time delays can occur purposefully or inherently in a wide range of engineering systems [12–14]. In general, time delays are common in control systems and can influence the stability of control systems. Even worse delays can occur when an adversary injects random TDS attacks into NCSs, making the systems inefficient or

even unstable. This circumstance stems from the fact that the controller needs to receive the measurement values in real time to be able to generate the control signals. NCSs transmit the sensor measurements from agents to a centralized control unit through communication channels, and injecting TDS attacks will result in instability in NCSs. Therefore, it is crucial to design a secure NCS that is robust to both natural delays and TDS attacks [3,15].

Even though it has been shown in the literature that TDS attacks can cause instability in NCSs [11], only a few studies have focused on detecting TDS attacks in real time, and none have investigated the compensation of TDS attacks by designing a secure controller. A neural network (NN) approach was developed in [16] as a tool for estimating a time delay in industrial communication systems with nonlinear dynamics, but the stability of this controller has not been investigated. Another NN-based approach was introduced in [17] to estimate the state of the system in real time. The aforementioned proposed algorithms require offline training and cannot detect TDS attacks in real time. Although machine learning techniques have been utilized for cyber attack detection in NCSs [18], various susceptible and erroneous detection results have been reported in the literature [19,20]. These machine learning methods are prone to maliciously altering the training or test data and cause disastrous operation issues and system instability [20]. A robust controller was introduced in [21] for systems with nonlinear dynamics. The proposed approach can compensate for the effects of TDS attacks in real time without detecting them. However, the proposed controller can only mitigate small amounts of TDS attacks. The approach proposed in [22] uses a neural-network-based detection algorithm to detect and estimate the TDS attack in real time. However, the proposed approach can estimate the TDS attacks accurately, but it cannot mitigate the effects of TDS attacks in real time. To mitigate the effect of a TDS attack, Ref. [12] proposed an adaptive control algorithm that estimates TDS attacks introduced into measurement signals. This work was able to detect and mitigate TDS attacks in real time. However, the stability of the proposed method was not investigated due to the nature of the controller design. Furthermore, the convergence of attack detection and estimation requires further investigation. Table 1 summarizes the advantages and disadvantages of approaches in the literature.

Table 1. The advantages and disadvantages of the approaches in the literature.

Approach	Advantage	Disadvantage
Machine-learning-based approaches [16–20]	These approaches do not require the dynamic model of the system	Stability analysis of neural network (NN)-based approaches is complex; offline learning time is required
Robust controller-based approach [21]	There is no need to detect attacks in real time	The system is not efficient due to its robustness to potential faults, failures, and attacks
NN-based detection approach [22]	Ability of detection and estimation of time-delay switch (TDS) attacks	Stability analysis requires further investigation; it cannot mitigate the effects of TDS attacks
Least-mean-square-based approach [12]	Accurate estimation of TDS attacks with a linear model of the system	Stability analysis is complex

The contributions of this papers are as follows:

- It develops a novel secure control strategy to estimate and compensate TDS attacks in real time for NCSs with linear dynamics to address the current barriers in the detection and compensation of TDS attacks in the literature.
- It designs a secure controller that is able to mitigate the effects of TDS attacks using the proposed model-based algorithm.
- The controller and estimator in this paper are designed based on the Lyapunov theory to guarantee the stability of an NCS under a TDS attack. The proposed method is compared with an NN-based method [22] to show the efficacy of the proposed technique in the presence of the TDS attack.

To summarize, the contribution of the paper is its proposal of a novel TDS attack detection technique along with its design of a secure Lyapunov-based controller for NCSs with linear dynamics under TDS attacks. The proposed algorithm is a model-based method that is able to detect and compensate for TDS attacks in real time with low computational complexity compared with learning-based methods.

The rest of the paper is organized as follows. Section 2 presents a general model for an NCS under a TDS attack. The proposed controller with a Luenberger observer is described in Section 3. Section 4 verifies the controller's stability. The case study is described in Section 5. Simulations and results are demonstrated in Section 6, and the conclusion is presented in Section 7.

2. Networked Control Systems

Despite all of the benefits of NCSs, including that they are fast, reliable, and have remote capability, NCSs are vulnerable to cyber disruptions and threats, since NCSs are highly dependent on information, communication, and cyber interfaces [1–3]. NCSs are used in critical infrastructures, and their security is categorized as one of the important concerns in the nation. Therefore, the vulnerability to external interruptions and attacks must be prevented. Since these systems heavily rely on networked communications, this dependency introduces delays, data packet drops, bandwidth allocations, and other cybersecurity issues in the data transfer process [11,23,24].

Specifically, delays can cause catastrophic failures in the systems that are under control. Measured data and control commands must be transferred within a limited period; otherwise, introducing delays to these signals makes the system unable to trace its operating conditions and causes an undesired response [3,25].

2.1. Dynamic Model of an NCS

A general diagram of an NCS system is presented in Figure 1. The communication between the plant and the controller takes place through a networked communication channel. Commands from the controller to the actuators and sensing signals from measurement sensors, which are vulnerable points of NCSs, must flow through the network. The NCS is mathematically represented by the following state-space model, assuming that the NCS has J agents:

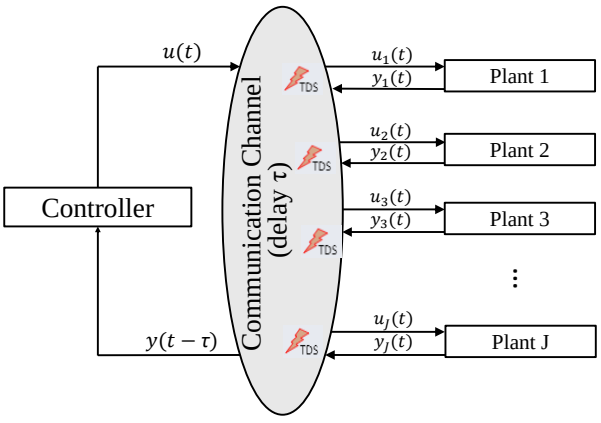

Figure 1. General diagram of a networked control system (NCS) with multiple plants under time-delay switch (TDS) attacks.

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t), \end{cases} \tag{1}$$

where $x(t)$ indicates the states of NCS and can be described as

$$x(t) = \begin{bmatrix} x_1(t)^T & x_2(t)^T & \cdots & x_J(t)^T \end{bmatrix}^T \tag{2}$$

and x_i is the state-space vector of the i_{th} agent of the NCS.

In a similar manner, $u(t)$ is the vector of inputs and $y(t)$ is the output, the aggregated state measurements of the system, which are described as

$$u(t) = \begin{bmatrix} u_1(t)^T & u_2(t)^T & \cdots & u_J(t)^T \end{bmatrix}^T \tag{3}$$

$$y(t) = \begin{bmatrix} y_1(t)^T & y_2(t)^T & \cdots & y_J(t)^T \end{bmatrix}^T. \tag{4}$$

Each agent in the NCS can have a different number of inputs $u_i(t)$, outputs $y_i(t)$, and states $x_i(t)$. This means that each vector in $x(t), u(t)$, and $y(t)$ has its own dimension.

$$x_i(t) = \begin{bmatrix} x_{i,1}(t) & x_{i,2}(t) & \cdots & x_{i,n_{xi}}(t) \end{bmatrix}^T \tag{5}$$

$$u_i(t) = \begin{bmatrix} u_{i,1}(t) & u_{i,2}(t) & \cdots & u_{i,n_{ui}}(t) \end{bmatrix}^T \tag{6}$$

$$y_i(t) = \begin{bmatrix} y_{i,1}(t) & y_{i,2}(t) & \cdots & y_{i,n_{yi}}(t) \end{bmatrix}^T, \tag{7}$$

where n_{xi}, n_{ui}, and n_{yi} are the dimensions of each vector of the state-space, inputs, and outputs, respectively, for the i_{th} agent.

The matrix A is described as:

$$A = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1J} \\ A_{21} & A_{22} & \cdots & A_{2J} \\ \vdots & \vdots & \ddots & \vdots \\ A_{J1} & A_{J2} & \cdots & A_{JJ} \end{bmatrix}. \tag{8}$$

Here, each sub-conjunct A_{ii} has the dimension $n_{xi} \times n_{xi}$ of the i_{th} agent in the system. A_{ab} represents the mutual dependency between agents.

If all the agents are independent of each other, the matrix changes to the following:

$$A = \begin{bmatrix} A_{11} & 0 & \cdots & 0 \\ 0 & A_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_{JJ} \end{bmatrix}. \tag{9}$$

In the same way, the matrix B is defined as

$$B = \begin{bmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B_J \end{bmatrix}. \tag{10}$$

Therefore, any single B_i has the dimension $n_{xi} \times n_{ui}$ based on the number of terms in the state vector (n_{xi}) and the number of terms in the input vector (n_{ui}) of the i_{th} agent in the NCS.

Matrix C is composed of C_i for each agent in the system. The dimension of each C_i is $n_{yi} \times n_{xi}$. Matrix C is defined as:

$$C = \begin{bmatrix} C_1 & 0 & \cdots & 0 \\ 0 & C_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & C_J \end{bmatrix}. \tag{11}$$

2.2. NCS under a TDS Attack

The controller of an NCS is considered to be an optimal controller, which is described as

$$u(t) = -Kz(t), \tag{12}$$

where z is the signal measured by the centralized controller.

Since delays are introduced to the communication channel, the signals received by the controller from each agent in the NCS are not the $y_i(t)$ originally observed from the system output. This paper assumes that an adversary cannot access control signals and only injects the TDS attacks into the measurement signals. The measured signal under a TDS attack can be described as

$$z_i(t) = y_i(t - \tau_i), \quad i \in \{1, 2, ..., J\}, \tag{13}$$

where τ_i is the delay of the i_{th} element of the NCS.

3. Controller Design: Lyapunov Compensation with a Luenberger Observer

3.1. Observer Design

A Luenberger observer is designed such that the error between the system measurement and estimated output converges to zero:

$$\begin{cases} \dot{\hat{x}} = Ax + Bu + L(y - \hat{y}) + \psi_2 \\ \hat{y} = C\hat{x} \end{cases}, \tag{14}$$

where the vectors $\hat{x}$, $\hat{u}$, and $\hat{y}$ are the state-space, the inputs, and the outputs of the observer, respectively. The compensator signal ψ_2 will be designed based on the subsequent stability analysis. The Luenberger gain L is a constant scalar number that multiplies the error between the output of the system $y = Cx$ and the estimated value from the observer $\hat{y} = C\hat{x}$.

Substituting the y and $\hat{y}$ elements in (14) yields

$$\begin{cases} \dot{\hat{x}} = A\hat{x} + B\hat{u} + LC(x - \hat{x}) + \psi_2 \\ \hat{y} = C\hat{x} \end{cases}. \tag{15}$$

Grouping the elements with $\hat{x}$, the system representation can be written as

$$\begin{cases} \dot{\hat{x}}(t) = (A - LC)\hat{x} + B\hat{u} + LCx + \psi_2 \\ \hat{y} = C\hat{x} \end{cases}. \tag{16}$$

The last term in Equation (16) is the response received by the observer from the plant through the delayed channel, which is actually $x(t - \tau)$. Given this variable, the state-space representation is changed to the following:

$$\begin{cases} \dot{\hat{x}}(t) = (A - LC)\hat{x} + B\hat{u} + LCx(t - \tau) + \psi_2 \\ \hat{y} = C\hat{x} \end{cases}. \tag{17}$$

3.2. Controller Design

The proposed control diagram is presented in Figure 2.

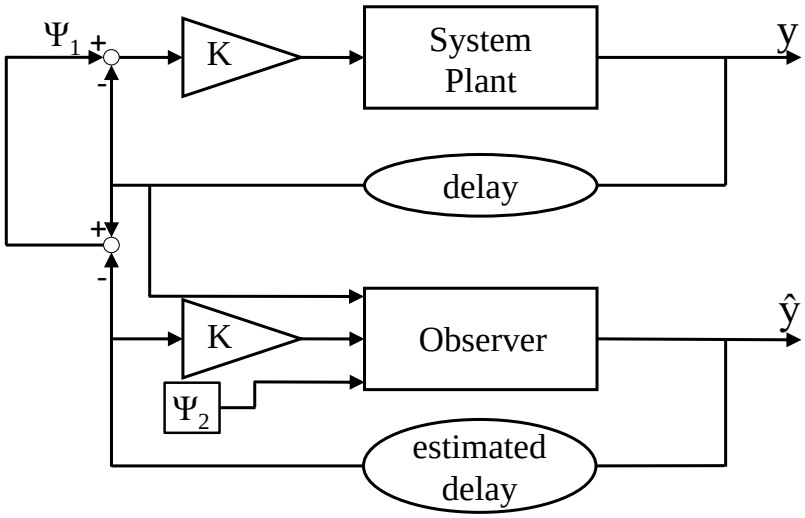

Figure 2. The proposed robust observer-based controller.

The delay presented in the superior feedback loop is the attack delay inserted into the system. The feedback controller is the same for both the plant and observer environment (K matrix). The terms of K must be defined to implement an optimal response to the system. It was used as a linear quadratic regulator (LQR) method to create the proper K matrix with the individual gains for each state in the system [26].

The delay in the system data is estimated at the feedback loop of the observer. This estimated delay signal is applied in the controller to adjust the control commands based on the inserted delay. The system model is set with an initial condition vector and the reference signal, which is a zero vector. It is replicated on the observer, and because of that, the inputs are $u = -Kx$ and $\hat{u} = -K\hat{x}$.

As seen in (18) and (19), the input signal of the system is affected by the delay in the communication channel. In the same way, the estimate delay is injected into the observer feedback response to also emulate the delay at the observer.

$$u = -Kx(t - \tau) + \psi_1 \tag{18}$$

$$\hat{u} = -K\hat{x}(t - \hat{\tau}) \tag{19}$$

As Figure 2 shows, ψ_1 compensates for the delay attack in the control input, and ψ_2 compensates for the delay attack in the observer process. These two terms will be further elaborated upon in the next section.

4. Proposed Delay Detection Method

In this section, ψ_1 and ψ_2 are designed using the Lyapunov approach. Furthermore, this section illustrates how TDS attacks are estimated in real time.

Consider the Lyapunov function described as

$$V_c = \frac{1}{2}\tilde{x}\tilde{x}^T + \frac{\alpha}{2}\tilde{\tau}\tilde{\tau}^T, \tag{20}$$

where α is a positive gain, $\tilde{x} \triangleq x - \hat{x}$ is the state estimation error, and $\tilde{\tau} \triangleq \tau - \hat{\tau}$ is the delay estimation error.

In (21), the derivative of the Lyapunov function is taken to obtain the required parameters and design a controller that is resilient against TDS attacks. It should be noted that

time-delay attacks here target the input signals u_{real} and u_{obs}. The output data y from the plant also have the delay attack shift in this model.

$$\dot{V}_c = \tilde{x}\dot{\tilde{x}}^T + \alpha\tilde{\tau}\dot{\tilde{\tau}}^T \tag{21}$$

Substituting $\dot{\tilde{x}} = (\dot{x} - \dot{\hat{x}})$ and $\dot{\tilde{\tau}} = (\dot{\tau} - \dot{\hat{\tau}})$ into (21), we obtain:

$$\dot{V}_c = \tilde{x}\{\dot{x} - \dot{\hat{x}}\}^T + \alpha\tilde{\tau}\{\dot{\tau} - \dot{\hat{\tau}}\}^T. \tag{22}$$

Then, $\dot{x}$ and $\dot{\hat{x}}$ are substituted according to (1) and (14), respectively. The equation changes into:

$$\begin{aligned}\dot{V}_c =& \tilde{x}\{Ax + Bu - ((A - LC)\hat{x} + B\hat{u} \\ &+ LCx(t - \tau) + \psi_2)\}^T + \alpha\tilde{\tau}(\dot{\tau} - \dot{\hat{\tau}})^T.\end{aligned} \tag{23}$$

Substituting the signals u and $\hat{u}$ from (18) and (19), the equation becomes the following:

$$\begin{aligned}\dot{V}_c = \tilde{x}\{&Ax + B(-Kx(t - \tau) + \psi_1) \\ &- (A\hat{x} + B(-K\hat{x}(t - \hat{\tau}) \\ &+ LCx(t - \tau) + \psi_2)\}^T + \alpha\tilde{\tau}(\dot{\tau} - \dot{\hat{\tau}})^T.\end{aligned} \tag{24}$$

Considering a constant delay in the channel, even if it happens over short periods of time, the derivative of the delay is going to be null ($\dot{\tau} = 0$). Using a Taylor series, the delayed signal is modeled approximately up to the first derivative term as $x(t - \tau) = x - \dot{x}\tau$.

$$\begin{aligned}\dot{V}_c = \tilde{x}\{&(A - LC)\tilde{x} \\ &- BK(x(t - \tau) - \hat{x}(t - \hat{\tau})) + B\psi_1 \\ &+ LC\dot{x}\tau - \psi_2\}^T - \alpha\tilde{\tau}(\dot{\hat{\tau}})^T\end{aligned} \tag{25}$$

Assuming that the second and third terms in (25) can cancel out each other, ψ_1 can be obtained as follows:

$$\psi_1 = K(x(t - \tau) - \hat{x}(t - \hat{\tau})). \tag{26}$$

After this, the derivative of the Lyapunov function is simplified as in (27).

$$\begin{aligned}\dot{V}_c = \tilde{x}\{&(A - LC)\tilde{x} \\ &+ LC(\dot{\hat{x}} + \dot{\tilde{x}})(\hat{\tau} + \tilde{\tau}) - \psi_2\}^T - \alpha\tilde{\tau}(\dot{\hat{\tau}})^T\end{aligned} \tag{27}$$

Applying the distributive property, Equation (27) is extended to (E:dem4):

$$\begin{aligned}\dot{V}_c = \tilde{x}\{&(A - LC)\tilde{x} \\ &+ LC(\dot{\hat{x}}\hat{\tau} + \dot{\hat{x}}\tilde{\tau} + \dot{\tilde{x}}\hat{\tau} + \dot{\tilde{x}}\tilde{\tau}) - \psi_2\}^T - \alpha\tilde{\tau}(\dot{\hat{\tau}})^T.\end{aligned} \tag{28}$$

Simplifying (27), we obtain the following equations, which will be used to find the estimated delay $\hat{\tau}$:

$$\tilde{x}LC(\dot{\hat{x}} + \dot{\tilde{x}})\tilde{\tau}^T = \alpha\tilde{\tau}(\dot{\hat{\tau}})^T \tag{29}$$

$$\dot{\hat{\tau}} = \frac{LC}{\alpha}(\dot{\hat{x}} + \dot{\tilde{x}})\tilde{x}. \tag{30}$$

The element α is a parameter for characterizing the system to make it possible to run the computation of the estimated delay value. Unfortunately, there is not a previous relation between the physical parameters of the system and the value of α. The moment when the attack is deployed and the amount of delay injected have different effects on the system. The method used to get α is based on the peak value observed when tracking the error signal—the difference between the plant response and the observer response—and defining the α value. Then, some series of tests must be performed under known TDS

attack conditions to validate the definition of α. An offset may be applied according to the essay results to guarantee more precise estimates.

ψ_2 is obtained below:

$$\psi_2 = LC(\dot{\hat{x}} + \dot{\tilde{x}})\hat{\tau}. \tag{31}$$

The Lyapunov theory is applied to guarantee that the system remains stable at different operating points. The Luenberger gain L must satisfy the following equation:

$$\tilde{x}\{(A - LC)\tilde{x}\}^T < 0. \tag{32}$$

The derivative $\dot{\hat{x}}$ can be taken from the observer. However, the error signal and its derivative $\dot{\tilde{x}}$ must be deduced—because it is not possible to measure data at the plant output before the delayed channel—by checking the error $x(t-\tau) - \hat{x}(t-\hat{\tau})$.

The Taylor series approximation must be considered; neglecting the higher-order terms, the delayed signal is represented by the following:

$$x(t-\tau) = x - \dot{x}\tau. \tag{33}$$

Similarly, the estimated states are obtained below:

$$\hat{x}(t-\hat{\tau}) = \hat{x} - \dot{\hat{x}}\hat{\tau}. \tag{34}$$

Subtracting Equations (33) from (34) will result in (36):

$$x(t-\tau) - \hat{x}(t-\hat{\tau}) = \tilde{x} - \dot{x}\tau + \dot{\hat{x}}\hat{\tau} \tag{35}$$

$$x(t-\tau) - \hat{x}(t-\hat{\tau}) = \tilde{x} - \dot{x}(\hat{\tau} + \tilde{\tau}) + \dot{\hat{x}}\hat{\tau}. \tag{36}$$

The term $\tilde{\tau}$ can be neglected because it is expected to go to zero due to the proper function of the proposed estimator. In this case, the Equation (36) becomes:

$$x(t-\tau) - \hat{x}(t-\hat{\tau}) = \tilde{x} - \dot{\tilde{x}}\hat{\tau}. \tag{37}$$

Considering that the system must be stable because the chosen value of L must guarantee the Lyapunov stability criteria, the Luenberger observer must bring estimation error signals in the form of $\tilde{x} = a.e^{-kt}$. Then, $\dot{\tilde{x}} = -k\tilde{x}$. Taking $k = 1$ (the effects of this k can be absorbed by α) to simplify the calculations, Equation (37) becomes

$$x(t-\tau) - \hat{x}(t-\hat{\tau}) = \tilde{x}(t)(1 + \hat{\tau}) \tag{38}$$

$$\tilde{x}(t) = \frac{x(t-\tau) - \hat{x}(t-\hat{\tau}))}{1 + \hat{\tau}}. \tag{39}$$

This way, it is possible to deduce $\tilde{x}(t)$ and its derivative $\dot{\tilde{x}}(t)$ used in Equations (30) and (31). They are obtained with the difference between consecutive samples in the digital readings.

5. NCS Case Study: Load Frequency Control Design for Power Grids

Load variation may create frequency oscillations and ultimately cause power grid instability. When the the grid load increases, the frequency decreases, and vice versa. Once a rapid load change is sensed, the electrical torque output is changed, which leads to a mismatch between the electrical and mechanical torques. This torque mismatch results in turbine speed changes that, in turn, cause frequency oscillations in the grid [27].

The load frequency control (LFC) of power systems is crucial in sustaining the grid frequency within a predefined range. LFC guarantees that the grid generators can properly maintain a balance between load and energy supply using the regulation of generators' set-points [27].

The mathematical model for an NCS applied to the power grid with several agents was developed in [12]. The mathematical model presented in Equation (1) with the x_i vector is defined as the following:

$$x_i(t) = [\Delta f_i(t)\ \Delta P_{g_i}(t)\ \Delta P_{tu_i}(t)\ \Delta P_{pf_i}(t)\ e_i(t)]^T, \tag{40}$$

where $\Delta f_i(t)$ is the frequency deviation, $\Delta P_{g_i}(t)$ is the generated power deviation, $\Delta P_{tu_i}(t)$ is the turbine position, $\Delta P_{pf_i}(t)$ is the tie-line power flow, and $e_i(t)]^T$ is the control error given by $e_i(t) = \int_0^t (\beta_i \Delta f_i + \Delta P_{pf_i})dt$.

Therefore, the equations are going to have $x_i(t)$, $u_i(t)$, and $y_i(t) \in \mathbb{R}^5$, where $u_i(t)$ is the control input vector, $x_i(t)$ is the state vector, and $y_i(t)$ is the output of the i_{th} agent in the system.

In this study, multiple grids are connected to the same tie-line within the same NCS. This means that agents can communicate with each other and exchange power among themselves through the grid. The matrix A will be similar to that presented in (8) with the following elements: Each A_{ii} will be

$$A_{ii} = \begin{bmatrix} \frac{-\mu_i}{J_i} & \frac{1}{J_i} & 0 & \frac{-1}{J_i} & 0 \\ 0 & \frac{-1}{T_{tu,i}} & \frac{1}{T_{tu,i}} & 0 & 0 \\ \frac{-1}{\omega_i T_{g,i}} & 0 & \frac{-1}{T_{g,i}} & 0 & 0 \\ \sum_{i=j,j=1}^{2} 2\pi T_{i,j} & 0 & 0 & 0 & 0 \\ \beta_i & 0 & 0 & 1 & 0 \end{bmatrix} \tag{41}$$

and A_{ij} will be

$$A_{i,j} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -2\pi T_{i,j} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{42}$$

The parameters presented in (41) and (42) are described as follows:

$$\begin{aligned} J_i &- \text{generator moment of inertia} \\ \beta_i &- \text{frequency bias factor} \\ \omega_i &- \text{speed-drop coefficient} \\ \mu_i &- \text{damping coefficient} \\ T_{g,i} &- \text{governor time constant} \\ T_{tu,i} &- \text{turbine time constant} \\ T_{i,j} &- \text{stiffness constant between } i_{th} \text{ and } j_{th} \text{ agents} \end{aligned}$$

Similarly to (10), the matrix B is defined below:

$$B_i = \begin{bmatrix} 0 & 0 & \frac{1}{T_{g,i}} & 0 & 0 \end{bmatrix}^T. \tag{43}$$

Since vectors $y(t)$ and $x(t)$ are the same as those shown in Equation (1), the matrix C presented in Equation (1) is an identity matrix, and finally, the matrix D is considered null in this study.

6. Simulation Results

This section illustrates the performance of the proposed secure control design along with the TDS attack detection technique through the case study that was introduced in Section 5. On top of the simulation, the method was implemented in a hardware-in-the-loop (HIL) environment to show that the proposed method is practical. For the HIL testing, we used a DS1104 Controller Board in connection with the MATLAB Simulink software. The LFC model was implemented via MATLAB Simulink 2019a, and it was converted into a C program to be loaded into the Dspace board. The results were observed using the Dspace console in real time. To show that the proposed method can perform well under measurement noise, we added zero-mean Gaussian noise during the HIL performance testing. As shown in Figure 3, the NCS, including two agents, was subjected to TDS attacks. Table 2 illustrates the parameter values that were used in the simulation.

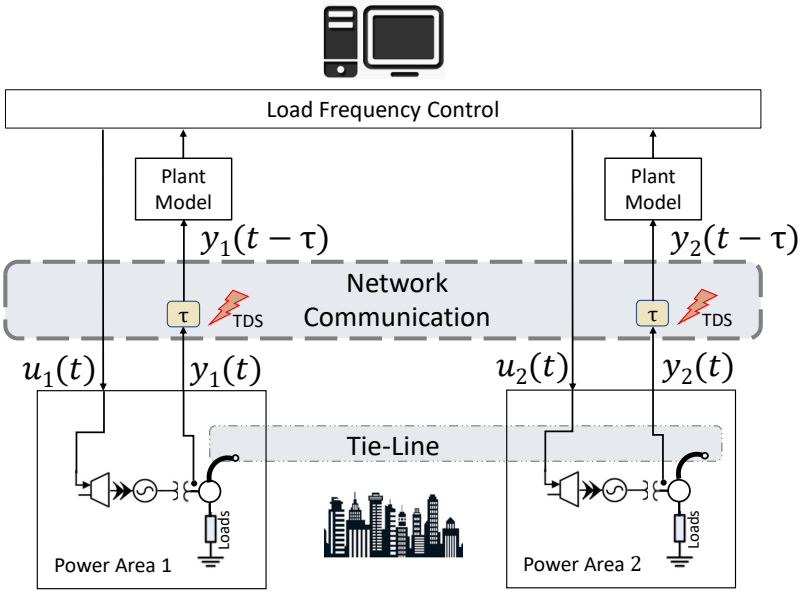

Figure 3. Two-agent load frequency control (LFC) system.

Table 2. Simulated Power Areas' Parameter Values

Description	Symbol	Power Area 1	Power Area 2
Generator Moment of Inertia	J_1	10	12
Frequency Bias Factor	β_1	21.5	21
Speed-Drop Coefficient	ω_1	0.05	0.05
Damping Coefficient	μ_1	1.5	1
Governor Time Constant	$T_{g,1}$	0.12 s	0.18 s
Turbine Time Constant	$T_{tu,1}$	0.2 s	0.45 s
Stiffness Constant *i-j*	$T_{1,2}$	0.198 pu/rad	0.198 pu/rad

The delay attacks were simulated based on the following assumptions:

Assumption 1.1. *The TDS attack takes place at a certain moment and remains constant.*

Assumption 1.2. *The TDS attack affects all the states. The starting moment and the delay period are the same for all the states.*

Assumption 1.3. *From the moment the attack is launched, it persists until the end of the simulation.*

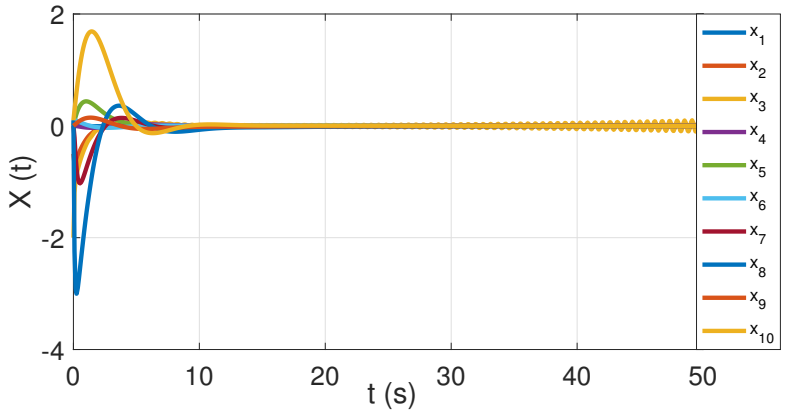

Figure 4. The NCS system under a TDS attack of $\tau = 0.19$ s at the instant $t_0 = 1$ s.

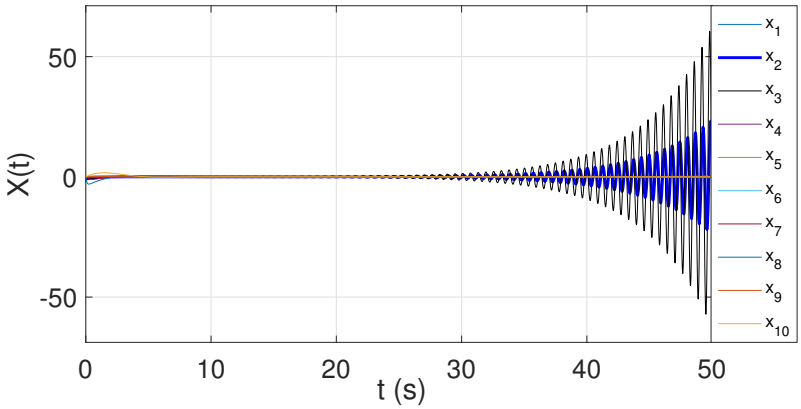

Figure 5. The NCS system under evaluation submitted to a TDS attack of $\tau = 0.20$ s at the instant $t_0 = 1$ s.

6.1. Vulnerability Analysis

When running the NCS in an optimal control situation, with no compensation algorithm to correct the delays, it can be observed that the system becomes unstable for attacks of $\tau = 190$ ms or higher. Figures 4 and 5 show the response of the system under a TDS attack. Both attacks were started at $t_0 = 1$ s, but the intensity of the attack is different. In the first case, $\tau = 0.19$ s, and in the other one, $\tau = 0.2$ s. It can be observed that the delay of 0.2 s had an aggressive effect on the system, leading the response to a divergent behavior with a highly increasing rate. Figure 4 represents a threshold condition, where the system started facing unstable responses due to the delay. It is possible to observe that the instability started around the instant at 30 s and the oscillations grew at a low rate. However, it was an unstable condition, and the system could not work under this attack. To detect and mitigate the effects of an attack, a resilient controller must be applied.

6.2. TDS Attack Detection and State Estimation

The observer compensation technique discussed in Section 4 made the system operate correctly, even with TDS attacks of around $\tau = 260$ ms. The same TDS attack as that shown in Figure 5 was simulated, but the system was equipped with the proposed secure controller. As Figure 6 shows, the adverse effect of the TDS attack was improved by the proposed state estimation mechanism.

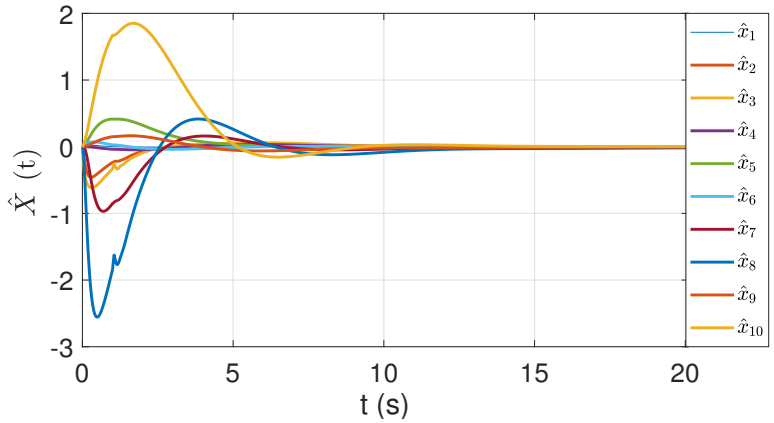

Figure 6. NCS system under a TDS attack of $\tau = 0.2$ s at the instant $t_0 = 1$ s with the Luenberger observer operating to compensate the errors.

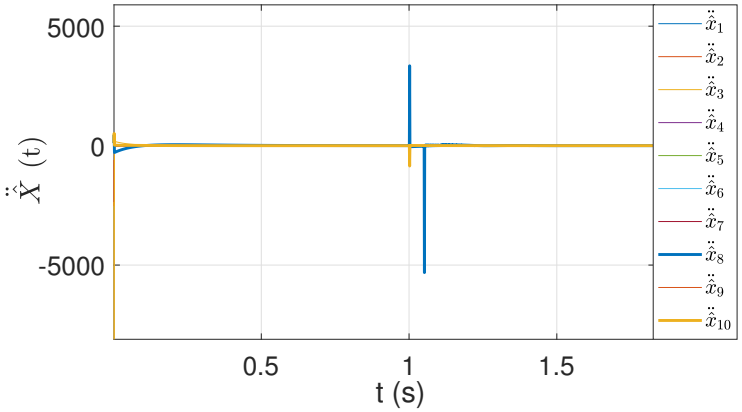

Figure 7. Second derivative of $\hat{x}$ used to detected the instant in time t_0 when the TDS is deployed.

The simulation was repeated with different time delays inserted by the TDS attack into the NCS at different starting instants ($t_0 = 1, 2, ..., 5$ seconds). Table 3 shows the results for three different time delays τ. The results show an Mean Square Error (MSE) around 5%.

Table 3. Delay estimation results—MSE.

τ (s)	$\hat{\tau}$ (s)	MSE (s)
0.15	0.1538	5.26%
0.22	0.2202	4.61%
0.26	0.2540	5.70%

The estimation of the delay depends on the parameter α mentioned in (30). The definition of α is a result of a complex set of essays running under known conditions to evaluate how the system responds to an injected delay depending on the amount of delay and the time instant at which was deployed. When an attack takes place, the error between the actual and the estimated states from the observer increases, and this is also reflected in the variations in $\hat{x}$. Using the second derivative of $\hat{x}$, the time instant of the TDS attack is detected (as shown in Figure 7). Thus, it is deployed, and the error is used to define the value to be chosen for α. The solution for computing α was created by using a constant value for alpha and then comparing the results with the offset that should be needed to get the correct values of $\hat{\tau}$. A polynomial approximation was created by taking the instant values of $\ddot{\hat{x}}$; then, it was incorporated in the α computation.

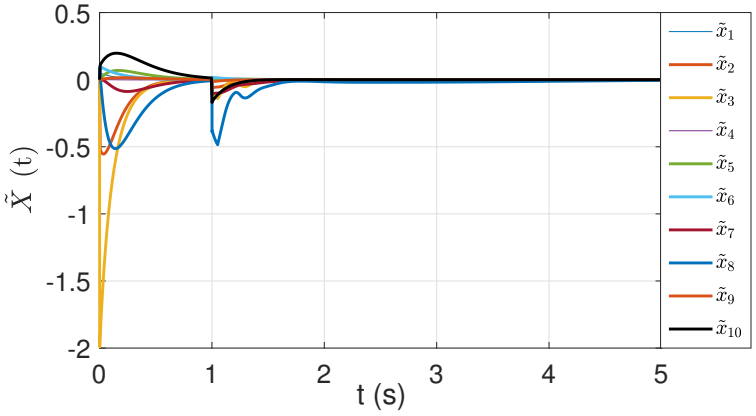

Figure 8. The state estimation error signal $\tilde{x}$ has a peak at the instant at 1 s, indicating that the attack was deployed. This peak value is used to estimate the proper α for $\hat{\tau}$ estimation.

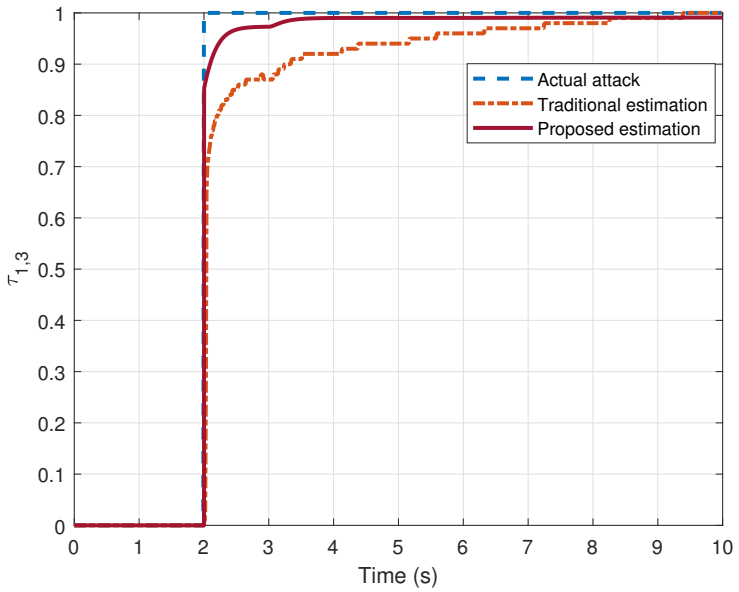

Figure 9. Delay estimation using the proposed method compared with the traditional method.

6.3. Performance Evaluation

The performance of the method proposed in this paper is compared with the performance of the control method presented in [22], which works based on an adaptive NN technique to estimate the time delay to which the NCS is exposed. The simulations were performed based on the following assumptions:

Assumption 2.1. *The delay attack takes place in a certain moment and remains constant.*

Assumption 2.2. *The delay attack targets only the state of* $x_3(t)$.

Assumption 2.3. *The attack persists from the moment it is launched until the end of the simulation.*

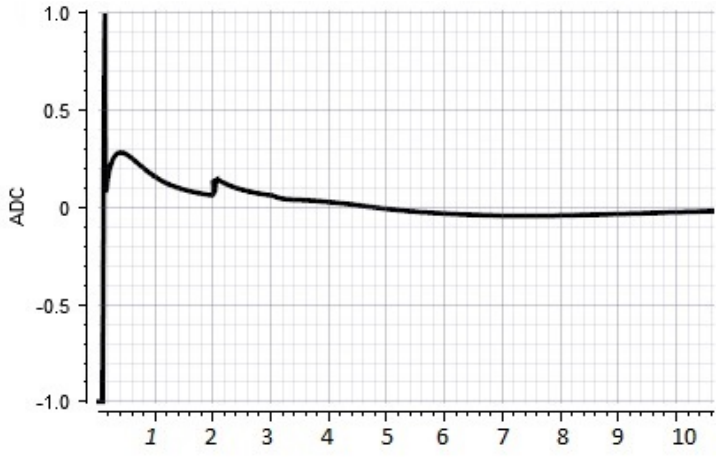

Figure 10. Response of x_3 with controller correction for a $\tau = 1.0$ s delay injected at $t_0 = 2.0$ s. The signal was observed in a Dspace input to simulate the input of the plant received through a feedback loop with a delay.

A delay $\tau = 1$ s was inserted from $t_0 = 2$ s. The state estimation errors are shown in Figure 8. The results show that the observer was able to accurately estimate measurement signals, even when the NCS was under TDS attacks. The results associated with the proposed method are presented in Figure 9. As shown in the figure, it is clear that the proposed TDS attack detection technique is more accurate than the NN-based (traditional) detection technique.

The NN approach allows consecutive computations in order to correct the estimation error and compensate frequency discrepancies in the LFC. The proposed method based on the Lyapunov theory presented in (20) depends on the parameter α, which is a characteristic quantity of the system, but it also depends on the instant the attack takes place. A study using the values of $\dot{\hat{x}}$, $\hat{x}$, and $\tilde{x}$ was used to calculate this parameter. So, the final value of $\hat{\tau}$ was reached more quickly, but a steady-state error can happen. The better the adjustment of the α parameter, the lower the steady-state error.

Another experiment to validate the Lyapunov method for avoiding TDS attack effects was made in a hardware-in-the-loop environment using external hardware equipment, the dSPACE CP1104 platform. A feedback loop was made for the x_3 state through the connection on the board. A time delay of $\tau = 1.0$ s affected the LFC, and the resilient performance of the proposed controller was seen in the results. The signal response on x_3 is shown in Figure 10. This test is important because it shows the effectiveness of the solution in a real-life system, demonstrating how the correction takes place to keep the system working properly, even when it is subjected to a TDS attack.

7. Conclusions

This paper presented an approach to providing adjustments to the input signal in an NCS structure in order to keep a plant working properly, even under a TDS attack. The compensation signal is defined based on the Lyapunov theory and a Luenberger observer. The proposed approach was evaluated through a case study in which a two-agent LFC system was monitored and controlled. The performance of the controller was validated in a hardware-in-the-loop simulation using the dSPACE platform to emulate the feedback loop of the NCS under TDS attacks. It should be noted that the proposed method can be applied to any NCSs, such as cooperative driving systems.

During the transient response of the system, the proposed delay estimation is more precise compared with other techniques in the literature. Furthermore, the controller and estimator were designed based on Lyapunov stability analysis, unlike other traditional techniques. When the most significant variations take place, it is possible to detect the peaks caused by the attack. The final portion of the transient response already has lower

variation, and it brings uncertainties to the estimation of $\hat{\tau}$. If the attack is deployed at an instant close to the starting point, the estimation is also affected because the observer will get the actual values from the plant. The variation in a delay over time is also a strong challenge for estimations, but this paper considered only constant delay attacks. Future work will enhance the proposed method to investigate time-variable TDS attacks. Although this paper focused on an NCS with dependent agents, the proposed method is general and can be used for a multi-agent system with independent dynamics.

Author Contributions: Methodology, M.V. and A.S.; Writing – original draft, M.V., A.S. and M.R.K.; Writing – review and editing, M.V., A.S. and M.R.K. All authors have read and agreed to the published version of the manuscript.

Funding: Partial support of this research was provided by the Woodrow W. Everett, Jr. SCEEE Development Fund in cooperation with the Southeastern Association of Electrical Engineering Department Heads and the National Science Foundation under Grant No. CNS-1919855. Any opinions, findings, and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the sponsoring agency.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

NCS	Networked Control System
TDS	Time-Delay Switch
DoS	Denial-of-Service
FDI	False Data Injection
NN	Neural Network
LQR	Linear Quadratic Regulator
LFC	Load Frequency Control
HIL	Hardware-in-the-Loop

References

1. Hespanha, J.P.; Naghshtabrizi, P.; Xu, Y. A Survey of Recent Results in Networked Control Systems. *Proc. IEEE* **2007**, *95*, 138–162. [CrossRef]
2. Yarali, A.; Rahman, S. Smart Grid Networks: Promises and Challenges. *J. Commun.* **2012**, *7*. [CrossRef]
3. Sargolzaei A.; Abbaspour A.; Al Faruque, M.A.; Eddin, A.S.; Yen, K. Security Challenges of Networked Control Systems. *Sustain. Interdepend. Netw. Stud. Syst. Decis. Control* **2018**, *145*, 77–95.
4. Abbaspour, A.; Mokhtari, S.; Sargolzaei, A.; Yen, K.K. A Survey on Active Fault-Tolerant Control Systems. *Electronics* **2020**, *9*, 1513. [CrossRef]
5. Lu, A.; Yang, G. Observer-Based Control for Cyber-Physical Systems Under Denial-of-Service With a Decentralized Event-Triggered Scheme. *IEEE Trans. Cybern.* **2019**, *50*, 4886–4895. [CrossRef] [PubMed]
6. Khalghani, M.R.; Solanki, J.; Solanki, S.K.; Khooban, M.H.; Sargolzaei, A. Resilient Frequency Control Design for Microgrids Under False Data Injection. *IEEE Trans. Ind. Electron.* **2021**, *68*, 2151–2162. [CrossRef]
7. Hosseinzadeh, M.; Sinopoli, B.; Garone, E. Feasibility and Detection of Replay Attack in Networked Constrained Cyber-Physical Systems. In Proceedings of the 2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 22–27 September 2019; pp. 712–717. [CrossRef]
8. Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. *IEEE Trans. Power Syst.* **2017**, *32*, 3317–3318. [CrossRef]
9. Long, H.; Wu, Z.; Fang, C.; Gu, W.; Wei, X.; Zhan, H. Cyber-attack Detection Strategy Based on Distribution System State Estimation. *J. Mod. Power Syst. Clean Energy* **2020**, *8*, 669–678. [CrossRef]
10. Li, F.; Yan, X.; Xie, Y.; Sang, Z.; Yuan, X. A Review of Cyber-Attack Methods in Cyber-Physical Power System. In Proceedings of the 2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP), Xi'an, China, 21–24 October 2019; pp. 1335–1339. [CrossRef]
11. Sargolzaei, A.; Yen, K.; Abdelghani, M. Time-Delay Switch Attack on Load Frequency Control in Smart Grid. *Adv. Commun. Technol.* **2013**, *5*, 55–64.
12. Sargolzaei, A.; Yen, K.K.; Abdelghani, M.N. Preventing Time-Delay Switch Attack on Load Frequency Control in Distributed Power Systems. *IEEE Trans. Smart Grid* **2016**, *7*, 1176–1185. [CrossRef]
13. Chaudhuri, B.; Majumder, R.; Pal, B. Wide-Area Measurement-Based Stabilizing Control of Power System Considering Signal Transmission Delay. *Power Syst. IEEE Trans.* **2004**, *19*, 1971–1979. [CrossRef]

14. Wu, H.; Tsakalis, K.; Thomas Heydt, G. Evaluation of Time Delay Effects to Wide-Area Power System Stabilizer Design. *Power Syst. IEEE Trans.* **2004**, *19*, 1935–1941. [CrossRef]
15. Ali, H.; Dasgupta, D. Effects of Time Delays in the Electric Power Grid. In *Critical Infrastructure Protection VI*; Butts, J.; Shenoi, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 139–154.
16. Tan, Y. Time-varying time-delay estimation for nonlinear systems using neural networks. *Int. J. Appl. Math. Comput. Sci.* **2004**, *14*, 63–68.
17. Sadeghzadeh, N.; Afshar, A.; Menhaj, M.B. An MLP neural network for time delay prediction in networked control systems. In Proceedings of the Chinese Control and Decision Conference, Yantai, China, 2–4 July 2008; pp. 5314–5318.
18. Karimipour, H.; Dehghantanha, A.; Parizi, R.M.; Choo, K.R.; Leung, H. A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids. *IEEE Access* **2019**, *7*, 80778–80788. [CrossRef]
19. Huang, L.; Joseph, A.D.; Nelson, B.; Rubinstein, B.I.; Tygar, J.D. Adversarial Machine Learning. In *Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence*; Association for Computing Machinery: New York, NY, USA, 2011; pp. 43–58. [CrossRef]
20. Pitropakis, N.; Panaousis, E.; Giannetsos, T.; Anastasiadis, E.; Loukas, G. A taxonomy and survey of attacks against machine learning. *Comput. Sci. Rev.* **2019**, *34*, 100199. [CrossRef]
21. Sargolzaei, A.; Yen, K.K.; Abdelghani, M. Control of Nonlinear Heartbeat Models under Time- Delay-Switched Feedback Using Emotional Learning Control. *Int. J. Recent Trends Eng. Technol.* **2014**, *10*, 85.
22. Abbasspour, A.; Sargolzaei, A.; Victorio, M.; Khoshavi, N. A Neural Network-based Approach for Detection of Time Delay Switch Attack on Networked Control Systems. *Procedia Comput. Sci.* **2020**, *168*, 279–288. [CrossRef]
23. Gupta, R.A.; Chow, M. Networked Control System: Overview and Research Trends. *IEEE Trans. Ind. Electron.* **2010**, *57*, 2527–2535. [CrossRef]
24. Boroojeni, K.G.; Amini, M.H.; Iyengar, S. Overview of the Security and Privacy Issues in Smart Grids. In *Smart Grids: Security and Privacy Issues*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 1–16.
25. Galli, S.; Scaglione, A.; Wang, Z. Power Line Communications and the Smart Grid. In Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010; pp. 303–308.
26. Patarroyo-Montenegro, J.F.; Salazar-Duque, J.E.; Andrade, F. LQR Controller with Optimal Reference Tracking for Inverter-Based Generators on Islanded-Mode Microgrids. In Proceedings of the 2018 IEEE ANDESCON, Santiago de Cali, Colombia, 22–24 August 2018; pp. 1–5. [CrossRef]
27. Elgerd, O. Control of electric power systems. *IEEE Control Syst. Mag.* **1981**, *1*, 4–16. [CrossRef]