Detection and Mitigation of Time Delay Injection Attacks on Industrial Control Systems with PLCs

Emrah Korkmaz, Matthew Davis(✉), Andrey Dolgikh, and Victor Skormin

Binghamton University, Binghamton, NY 13902, USA
{ekorkma1,mdavis7,adolgikh,vskormin}@binghamton.edu

Abstract. National security agencies are increasingly concerned about cyber threats to Industrial Control Systems (ICS). For this reason, the detection and mitigation of cyber-attacks on ICS, as well as addressing the consequences of these attacks, are extensively researched. This paper describes the efforts of the cyber research team at Binghamton University that created an experimental cyber research testbed, designed as a power station equipped with low-watt electric machinery and industrial control and sensory systems, common in modern ICS. This paper presents a comprehensive study of time delay injection attacks on networked control systems, in which an attacker injects extra time delays into the feedback and forward channels of control systems. These attacks enable the adversary to interfere with the control system and create system instability, causing anomalous operational regimes and potentially forcing the system to crash. A technology based on an online recursive estimation of network time delays is proposed and validated by simulation studies and experiments on the testbed to mitigate any time delay injection attacks.

Keywords: Industrial control systems · Cyber-Physical systems · Testbed · Cyber-Security · Time delay injection attack · Time delay detection

1 Introduction

A recently published report by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) indicates that many organizations have Internet-connected control systems and are not even aware that they are directly accessible from the Internet [1]. Recently, industrial communication technologies are being moved on top of the standard Ethernet/TCP/IP stack of protocols [2]. Using Ethernet protocols in ICS provides benefits such as expanding the functionality of control devices, allowing remote control, and utilizing virtual machines within the network. Technology products, such as remote Human Machine Interface (HMI) software on smartphones or tablets enable operators to manage ICS remotely. Although these advantages enable control systems engineers to build cost-effective and user-friendly ICS, this networked connectivity opens doors to a massive amount of cyber-attacks targeting the ICS [3]. To prove this point, we successfully deployed a time delay injection attack on our laboratory testbed. The impact of this time delay injection attack on an ICS was examined, and a method of using recursive delay

J. Rak et al. (Eds.): MMM-ACNS 2017, LNCS 10446, pp. 62–74, 2017.
DOI: 10.1007/978-3-319-65127-9_6

estimation was implemented to accurately determine the injected time delay length within a short time period from the time of injection.

The rest of this paper is structured as follows: Sect. 2 presents the background of this research. Section 3 describes the designed testbed architecture and gives information about the Internet connection components. In Sect. 4, the effect of the time delay attack injection on ICS is discussed. Section 5 presents the recursive estimation based time delay detection technique and the obtained results. Finally, Sect. 6, contains the conclusions and further research on this topic.

2 Related Research

Over the past two decades, there was no lack of publications addressing time delays in ICS as well as demonstrating various control approaches [4–6]. Although most strategies were well justified by control theory and offered viable solutions, these solutions were not developed in the context of cyber-security. For instance, the authors in [7] present a discrete-time jump system approach in which a V-K iteration algorithm was utilized to design stabilizing controllers. However, the controller design was performed under the assumption that there were random and bounded delays between the sensor and the controller which is not always true for malicious delays. Another approach [8] addresses tuning the PID controller by PLC programming, based on models of unstable processes with a random time delay. This research is somewhat relevant to our study; however, the described stability conditions may not be sufficient for purposely designed time delay injection attacks. The authors in [9] propose gain scheduling for a PID controller to compensate for extra time delays in the system; however, control system stability cannot be assured for random delay values. Due to this lack of existing literature about the cyber-security implications of time delays in ICS, a cyber-security study of time delay attacks is performed for ICS in this paper.

There are several implementations and interpretations of network time delay attacks in literature. Larsen in [10] describes a time delay attack as a stale data attack. The attacker manipulates the timing of encrypted packets on the associated network, resulting in a difference between the physical and logical states of the process. Consequently, the control system may be driven to an arbitrary state. Krotofil et al. [11] suggest that for an effective stale data attack to drive the system to an unsafe condition, the adversaries must determine the optimal time duration of the attack. The researchers introduce this type of attack as a wormhole attack. With this attack method, an adversary establishes a link between the network nodes and can create delays over the network to drop packets maliciously [12, 13].

Time delay injection attacks on power systems are not uncommon. An adversary could exploit vulnerabilities along the communication links, which would cause the loss of critical information, and therefore unstable operation conditions can result [14]. The authors in [15] indicate that a time delay switch (TDS) attack can be performed to sabotage and degrade the performance of a smart grid. In another study, the authors propose a time delay detection mechanism to mitigate these attacks and introduce a modified controller in the case of a time delay injection [16]. This controller is only designed to control the power grid and the time delay injection is performed only in the feedback channels of the control system. However, in many cases the time delay can be injected into both the feedback and forward channels of the control network.

3 Industrial Control System Security Testbed

The ICS Security testbed built at Binghamton University features a digital control system that could typically be found in a power generation station at fossil fuel or nuclear power plants, electric grid, etc. The testbed is suitable for the deployment of typical cyber-attacks and the detailed monitoring of system operations, thus providing researchers with an unlimited amount of critical data [17]. The testbed components can be broken down into five categories:

3.1 Physical System

This equipment is used to investigate the effects of cyber-attacks on power generation hardware in two different power generation setups. The first unit is composed of a 0.25 HP 3-phase AC motor and a 0.33 HP permanent magnet DC motor which are connected via a coupling tie-in shaft. The PowerFlex 525 AC Drive controls the RPM of this motor-generator assembly. A series of single-phase loads are attached to the DC generator to safely dissipate the power, thereby protecting the system from overload conditions. The second power generating unit operates a 3-phase AC blower motor that drives a 12 V DC generator through airflow-based coupling. The airflow can be restricted externally thus simulating disturbance effects on air handling port. A separate PowerFlex 525 AC Drive is used to control the electrical power provided to the AC blower motor-generator module to manipulate the motor speed.

3.2 Measurement Devices

An Allen-Bradley 1794 Flex I/O module functions as a monitoring device for both power generation units. The power output of both the DC motor and the DC blower motor are connected to inputs of the Flex I/O, which then measures the voltage. Information about these voltages is transmitted to the ControlLogix controller which uses this information to display the values in the HMI as well as potentially alter the PowerFlex PID parameters to adjust the generated voltage.

3.3 Programmable Controllers

The testbed contains two different types of PLCs: an Allen-Bradley ControlLogix, which is an advanced controller, and an Allen-Bradley Micro850, which is a simpler multiple-IO controller. The ControlLogix 1756-L61 PLC is used as the central controller. Programming the ControlLogix device can be done using Rockwell Automation's RSLogix 5000 software. The power dissipation from the direct-coupled power generation unit is controlled by programming the Micro850 controller to alter the distribution of power to various single phase loads and a small DC motor. Rockwell Automation's Connected Components Workbench software is used to create the ladder logic diagrams for programming the Micro850.

3.4 Communication Infrastructures and Software

The components on the testbed communicate over the testbed network using the EtherNet/IP protocol and Common Industrial Protocol (CIP). To perform time delay injection attacks on the testbed, a traffic shaping VM is deployed on the testbed network. It is implemented via FreeBSD and DummyNet software [18]. This VM allows DummyNet-enabled bridges to be created using the existing PC hardware without disrupting any existing software installations of ICS components [19].

3.5 Scada-HMI

Human machine interface (HMI) systems permit operators to visualize and manipulate the testbed operations. On this testbed, the operator can observe and adjust the real-time output voltages of both power generation units. Proficy HMI/SCADA iFIX software is used to build, monitor, and control the entire HMI system.

4 Time Delay Injection Attack

The inherent time delay in ICS, perceived as a system stability issue, was addressed in various comprehensive studies [20–22]. However a time delay, when purposely designed and injected into the system by an adversary, is an effective method of attacking the network. For cyber-physical systems (CPS), packet delays on the control network might result in the deterioration of system performance and the loss of stability. Typical information technology (IT) computers and networks do no suffer from this timing criticality, therefore time delays on ICS networks deserve special attention.

The time delay can be created on both the forward and feedback channels of the control system (see Fig. 1). As described in the previous section, the PowerFlex drives and the measurement device are connected to the ICS network. While the PLC

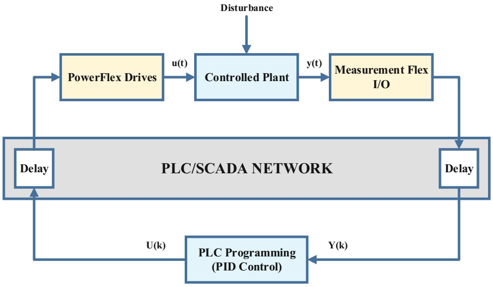

Fig. 1. Closed-loop diagram of testbed

communication with the PowerFlex drives is through the forward channel, the communication with the measurement devices is through the feedback channel.

4.1 Attack Model

Understanding the attack model and the threat scenario is important for preventing control system attacks. An attacker with network access can influence and disrupt the basic control functions, rather than only the longer-term controls commonly associated with a SCADA environment. Although simple time delay attacks do not require any expert knowledge, in many stale data attacks the attackers must directly manipulate the integrity of communications between field devices and controllers [11]. To execute a successful time delay injection attack, the adversary needs to conduct extensive reconnaissance work to identify the data flow of the control network which consists of sensors, controllers, and motor drives. To successfully exploit the network vulnerability, the attacker can use a network traffic shaping tool to create arbitrary delays within the targeted control network. As seen in Fig. 2, the attacker's computer is deployed on the testbed, which facilitates an experimental investigation of the ways and means of data traffic manipulation in the attacked control network. It is safe to assume that the attacker gains access to the control network and can inject time delays into the communication channels. Consequently, the immediate measurement of the desired process output Y(t) and the output of the actuators U(t) will be replaced by delayed ones,

$$Y^{DEL}(t) = Y(t - \tau) \text{ and } U^{DEL}(t) = U(t - \tau) \quad (1)$$

where τ is the desired delay magnitude, defined by the attacker.

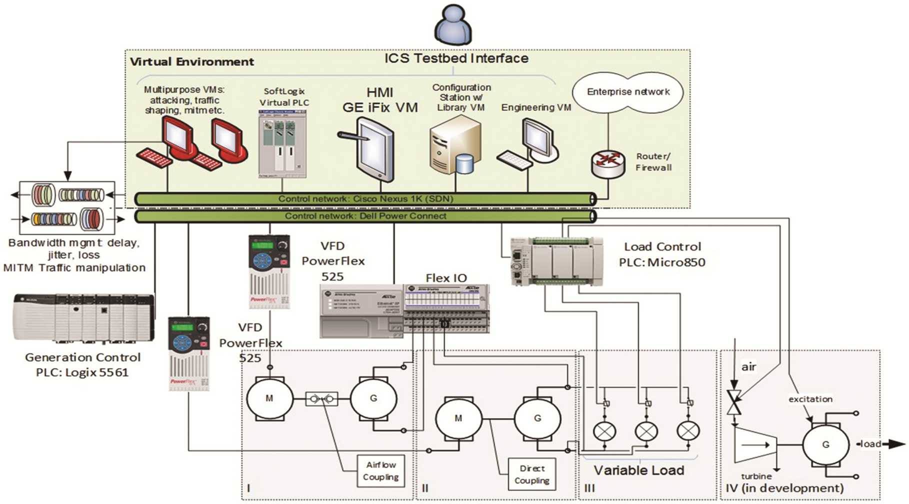
Virtual Environment
ICS Testbed Interface
Multipurpose VMs: attacking, traffic shaping, mitm etc.
SoftLogix Virtual PLC
HMI GE iFix VM
Configuration Station w/ Library VM
Engineering VM
Enterprise network
Router/ Firewall
Control network: Cisco Nexus 1K (SDN)
Control network: Dell Power Connect
Bandwidth mgmt delay, jitter, loss
MITM Traffic manipulation
Generation Control PLC: Logix 5561
VFD PowerFlex 525
VFD PowerFlex 525
Flex IO
Load Control PLC: Micro850
M
G
Airflow Coupling
I
M
G
Direct Coupling
II
Variable Load
III
air
excitation
turbine
G
load
IV (in development)

Fig. 2. Testbed architecture

The magnitude of the delay injected by the attacker must be chosen carefully because the added delay in the control system can be detected by the ICS and the sensor control code. If such a delay is detected by the devices on the network, the devices will automatically enter a fault condition which halts the system. However, the extra delay cannot be detected if it is injected gradually and each increment does not exceed the maximum change in delay value that would invoke the termination procedure in the system. We believe this is due to delay adaption code built into the network's enabled sensors that reacts to sudden significant delay increments but adapts to small ones.

4.2 Time Delay Attack

The testbed was configured to maintain a specified output voltage under varying load conditions to investigate the effectiveness of time delay attacks. This function was realized via a PID based controller in the feedback control loop. The blower motor's set point voltage value was chosen as 1.9 volts, which is small enough to protect attached devices from any potential overvoltage problems. The direct-coupled motor-generator module of the testbed operated at a frequency proportional to that of the blower motor. The direct-coupled motor-generator module can generate voltages up to 400 volts, and thus its voltage control is paramount because of the overvoltage values that might occur and potentially damage attached devices.

Detectable Delays

First, a time delay attack on the testbed with a 100 ms delay was deployed. It was detected almost immediately by the devices on the network, resulting in fault conditions on the PowerFlex drives and stopping the motor-generator modules. The experiments showed that the extra delay causes connection time outs and clears the data table of the drive so that the networked drives are no longer under the control of the PLCs. If the operators of the ICS encounter "communication interrupted" fault codes stemming from a time delay attack, they are to perform system debugging and effectively mitigate the problem. However, the "connection time outs" are a very common issue in a variety of interconnection protocols [23], and the time delay attack cannot be easily identified as the source of the fault. Although this attack method can be perceived as an ineffective way to stop a power generation unit, if it is conducted on a real power plant it may cause blackouts in a large portion of the electric power grid, depending on the specific configuration of each controller at each facility/unit and the type of the process.

Undetectable Delays

The EtherNet/IP based devices can also be subjected to a gradual time delay attack. This attack allows for much larger delays to be introduced without detection. Consider the graphs featured in Fig. 3. The upper graph depicts the output frequencies of the PowerFlex drives while the lower graph shows the measured output voltage of the air blower motor-generator module. In this experiment, during the first 100 s there was no network delay in either the feedback or forward channels. For the time delay attack to be successful, it must begin with subtle delay values that should be increased gradually over time. Thus every 10 s the delay value was increased by an additional 10 ms. In this case, the PowerFlex drives and PLC computers do not generate any fault conditions and give no indication of the time delay increase. The delay in the network prevents the PLC PID block from observing the actual process conditions and prevents the generation of timely control efforts [24]. The internal data table of the controller is supposed to update its input tags and output values based on the configured requested packet interval (RPI) parameter. However, the controller does not update the input and output data with the desired RPI. Instead, it updates all data at the maliciously altered time delay interval. It could be seen that the RPI value of 10 ms does not allow for the detection of small delay increments under 10 ms [25]. Consequently, the control task is still carried out by the PLC and PowerFlex drives, but the desired control performance is not achieved. This loss of desired control performance results in oscillations of the PID response due to the network delay, which effectively increases the dead time of the process and invalidates the tuning of the PID controller. When the controller is improperly tuned, it fails to dampen the oscillatory process in the control loop.

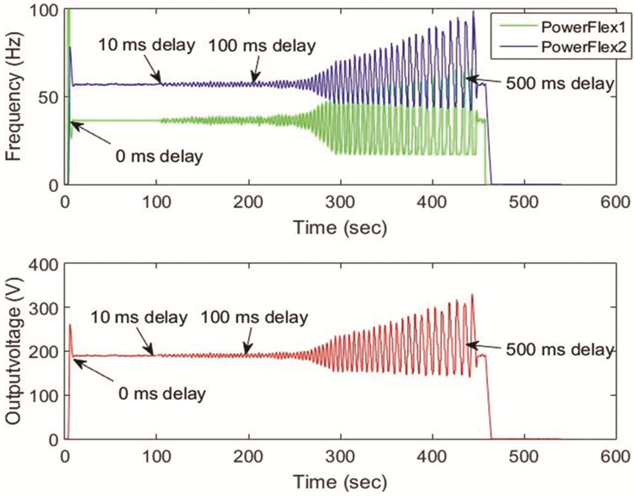

Fig. 3. Measured output voltage and frequency values of drives

At each cycle, the amplitude of the oscillation increases and eventually exceeds the operational safety limits. An overvoltage condition is forced by this time delay attack and causes the system to produce a very high output voltage (over 300 volts). As the delay increases, the stale data becomes a dominant factor in the control loop instability. It was noticed that as the time delay exceeds 150 ms, the system becomes unstable; with a delay of approximately 500 ms, the system crashed, burning out all the light bulbs that functioned as a resistive load for the direct-coupled generator.

It should be noted that having the testbed offers the “attackers” the luxury of having information crucial for the deployment of a successful attack. Although real attackers will not be able to determine attack parameters yielding the desired impact based on system configuration and PID response, the information required to design a time delay attack can be obtained from open sources, such as Wikipedia, data sheets, companies, and various side channels. If an attacker has access to the network, the task becomes trivial. The attack can also be mounted blindly by slowly ramping up the delay value.

5 Mitigation Technique

Literature presents many mitigation and control techniques for time delayed ICS [7–9]. While many of them offer a valid approach to dealing with time delays in ICS, they cannot be easily implemented with a real-world PLC. In this paper, we propose a novel, simplistic but very functional, time delay detection approach and validate it with a Simulink model and through actual implementation for a PLC.

5.1 Simulation Setup

A multiple model approach for the detection of various time delays in the control systems is proposed. After implementing and testing in the Simulink environment, it was implemented and tested on a PLC. Modeling the peculiarities of a real-world PLC and digital IO in such a way that the output of the Simulink model was consistent with the real PLC proved to be difficult. The modeling addressed issues such as the nonlinear behavior of the blower, unknown dead zones, motor ramp up, breaking curves, high system inertia, etc. The model development, validation, parameter estimation, and tracking was based on the techniques suggested in [22].

The detection methodology can be explained as follows. Assume that $R(t), Y(t), Y^{OBS}(t)$ and $Y^{MOD}(t)$ are correspondingly the input, output, observed output, and modeled output of a dynamic channel of an ICS. It is understood that $Y(t) = F[R(t)]$ is the input-output relationship describing the dynamic channel that reflects the relevant physical phenomena. Due to the delay in the information channel, τ, the observed output is $Y^{OBS}(t) = Y(t - \tau) \neq Y(t)$. For this reason, a mathematical model based on the system input $R(t)$ and observed output $Y^{OBS}(t)$, $Y^{MOD}(t) = \Phi[R(t)]$ would not properly represent the relationship $Y(t) = F[R(t)]$. Consequently, $Y^{MOD}(t)$ will differ from $Y(t)$. One can easily establish that the coefficient of determination of the model $Y^{MOD}(t) = \Phi[R(t)]$ is expected to be low [22]. Now consider mathematical models $Y^{MOD}\left(t, T_j\right) = \varphi\left[R\left(t - T_j\right)\right]$, built based on the system input $R(t - T_j)$ and the observed output $Y^{OBS}(t)$, where $T_j, j = 1, 2, 3, \ldots$ is one of the several alternative delays inserted in the channel of the input variable $R(t)$. It is understood that the most accurate model, resulting in the minimum discrepancy between $Y^{OBS}(t)$ and $Y^{MOD}\left(t, T_j\right)$ or the largest value of the coefficient of determination, is the one where delays T_j and τ have close numerical values. The principle of operation of the delay estimation procedure is shown in Fig. 4.

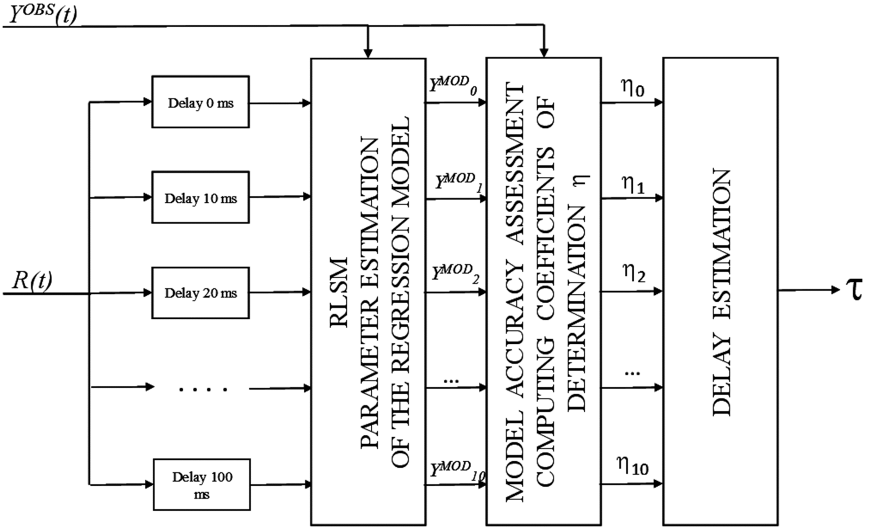

Fig. 4. RLSM model approach for different delay values

To implement this approach, first a mathematical model $Y^{MOD}\left(t, T_j\right) = \varphi\left[R\left(t - T_j\right)\right]$ was developed for the no-delay conditions in the form of a Z-domain transfer function

$$\frac{Y^{OBS}(z)}{R(z)} = \frac{b_2 z^{-1} + b_1 z^{-2} + b_0 z^{-3}}{1 + a_2 z^{-1} + a_1 z^{-2} + a_0 z - 3} \tag{2}$$

or in the discrete-time domain (where i = 1, 2, 3, … is the discrete-time index):

$$Y^{OBS}(i) = -a_2 Y^{OBS}(i-1) - a_1 Y^{OBS}(i-2) - a_0 Y^{OBS}(i-3) + b_2 R(i-1) + b_1 R(i-2) + b_0 R(i-3) \tag{3}$$

It has been established that the third order of the model is sufficient for the accurate description of the dynamic channel in question. Further increases in the order of the model practically do not increase the value of the coefficient of determination. It could be seen that the discrete-time version of the model is a regression equation, with input variables X, output variables Y, and parameters A, defined in Eq. (4). $\Delta = 10$ ms is the time step of the discrete-time control/monitoring procedure of the testbed. Parameters of this equation were estimated using the Least Squares Method.

$$X(t) = \begin{bmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \\ x_4(t) \\ x_5(t) \\ x_{6[}(t) \end{bmatrix} = \begin{bmatrix} Y^{OBS}[(i-1)\Delta] \\ Y^{OBS}[(i-2)\Delta] \\ Y^{OBS}[(i-3)\Delta] \\ R[(i-1)\Delta] \\ R[(i-2)\Delta] \\ R[(i-3)\Delta] \end{bmatrix}, Y^{OBS}(t), \text{and}\, A = \begin{bmatrix} a_2 \\ a_1 \\ a_0 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} \tag{4}$$

Upon the completion of the parameter estimation task for the no-delay model, the procedure runs the RLSM for the parameter estimation of the ten models that include various delay magnitudes, and the parameters of the no-delay model are utilized as the starting parameter values. Now input variables X and output variables Y are shown in Eq. (5) where T_j is the delay value inserted in the j-th model, $j = 1, 2, 3, \ldots, 10$.

$$X(t) = \begin{bmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \\ x_4(t) \\ x_5(t) \\ x_{6[}(t) \end{bmatrix} = \begin{bmatrix} Y^{OBS}[(i-1)\Delta] \\ Y^{OBS}[(i-2)\Delta] \\ Y^{OBS}[(i-3)\Delta] \\ R[(i-1)\Delta - T_j] \\ R[(i-2)\Delta - T_j] \\ R[(i-3)\Delta - T_j] \end{bmatrix} \text{ and } Y^{OBS}(t) \tag{5}$$

The validity of the RLSM-supported models is periodically checked by computing the appropriate coefficients of determination, and the model with the highest value of the coefficient of determination or the lowest variance of the modeling error points at the most accurate estimate of the delay injected in the network. This RLSM model has been successfully implemented in the Simulink software and applied to the simulated ICS featuring the testbed, as seen in Fig. 5. Thus, the system operator could be alerted to the presence of a potentially unnoticeable network delay that is still capable of altering the system dynamics, and the operator can assess the delay magnitude so that timely precautions can be taken against the time delays on the control systems. Also, the knowledge of the time delay can be used to drive a gain scheduling procedure for the main PID controller. This way the stability of the control system and its performance can be maintained at an acceptable level even under attack [9].

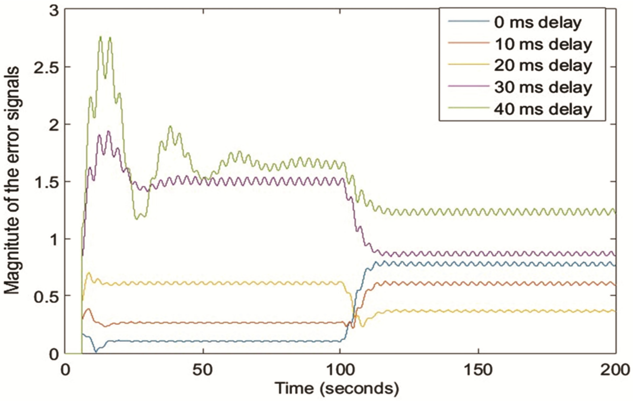

Fig. 5. Time delay detection

5.2 Experimental Implementation

Experimental implementation and testing is the optimal way to demonstrate the feasibility and efficiency of the described technology. Therefore, the delay detection/estimation approach, implemented in PLC code, was deployed on the testbed and utilized the "real" testbed data. First, a third order "no-delay" model was established thus providing starting parameter values to ten tunable regression models. A finite-memory RLSM procedure [22] was employed for parameter tuning of the individual models. As per Fig. 5, a provision was made for the assessment and display of the accuracy of the individual models. During the first 100 ms "no-delay" operation of the testbed only one model, describing the no-delay system showed a very low variance of the modeling error, associated with the measurement noise. After 100 s, a 20-ms delay was injected into both network channels of the control system. At this point, the variance of the modeling error began changing. Within about 10 s of the delay injection, the magnitude of the delay was accurately determined. Given that ICS are so time critical, accurately determining the time delay within a short time from injection is critical for the system's optimal operation. Since this ICS testbed operates as a fully functioning ICS, the results of this experiment are not limited to only this testbed as this technology can be successfully applied to any general ICS.

6 Conclusion and Future Work

In this paper, a time delay injection attack was deployed on both the forward and feedback channels of an ICS testbed. The results show that small delay values on control systems are not detected by system devices and their effects are minimal for the testbed. However, gradually increasing time delays may force the control system into an unstable state. The results of this research can be summarized as follows:

- A practical detection approach for time delay attacks on a PLC controlled, continuous process is formulated.
- A bank of models is built by monitoring a real controlled plant and capturing its dynamics using the recursive least squares method (RLSM).
- The approach operates by assessing the individual accuracy of the bank of models describing the real controlled plant with various delays in the loop.
- The approach was successfully implemented and tested in the Simulink environment and the testbed environment.

Future work for this research includes real-time implementation of the described technology in conjunction with a gain scheduling system for a PLS based controller.

Acknowledgement. This research was funded in parts by the Air Force Office of Scientific Research grant "Semantic Approach to Behavior Based IDS and its Applications" (Number FA9550-12-10077) and by the Office of Naval Research grant "Security Approach for Industrial Control Systems" (Number N00014-15-1-2759).

References

1. ICS-CERT monitor. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERTMonitorMay-Jun2015.pdf. Accessed 14 July 2016
2. Antonioli, D., Tippenhauer, N.O.: Minicps: a toolkit for security research on cps networks. In: Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or Privacy, pp. 91–100. ACM (2015)
3. Cruz, T., Barrigas, J., Proença, J., Graziano, A., Panzieri, S., Lev, L., Simões, P.: Improving network security monitoring for industrial control systems. In: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 878–881. IEEE (2015)
4. Fan, W.-H., Cai, H., Chen, Q.-W., Hu, W.-L.: Stability of networked control systems with time-delay. Kongzhi Lilun yu Yingyong/Control Theory Appl. (China), **21**(6), 880–884 (2004)
5. Michiels, W., Niculescu, S.-I.: Stability, control, and computation for time-delay systems: an eigenvalue-based approach, vol. 27. Siam (2014)
6. Wang, F.-Y., Liu, D.: Networked control systems. Springer, London (2008)
7. Xiao, L., Hassibi, A., How, J. P.: Control with random communication delays via a discrete-time jump system approach. In: Proceedings of the 2000 American Control Conference. vol. 3, pp. 2199–2204. IEEE (2000)
8. Lee, Y., Lee, J., Park, S.: PID controller tuning for integrating and unstable processes with time delay. Chem. Eng. Sci. **55**(17), 3481–3493 (2000)
9. Gupta, R.A., Chow, M.-Y.: Performance assessment and compensation for secure networked control systems. In: 34th Annual Conference of IEEE Industrial Electronics. IECON 2008, pp. 2929–2934. IEEE (2008)
10. Larsen, J.: Controlling without modifying: the stale data problem. In: S4x16, Miami, US, January 2016
11. Krotofil, M., Cardenas, A., Larsen, J., Gollmann, D.: Vulnerabilities of cyber-physical systems to stale data: determining the optimal time to launch attacks. Int. J. Crit. Infrastruct. Prot. **7**(4), 213–232 (2014)
12. Lee, P., Clark, A., Bushnell, L., Poovendran, R.: A passivity framework for modeling and mitigating wormhole attacks on networked control systems. IEEE Trans. Autom. Control **59**(12), 3224–3237 (2014)
13. Hu, Y.-C., Perrig, A., Johnson, D.B.: Wormhole attacks in wireless networks. IEEE J. Sel. Areas Commun. **24**(2), 370–380 (2006)
14. Sridhar, S., Hahn, A., Govindarasu, M.: Cyber–physical system security for the electric power grid. Proc. IEEE **100**(1), 210–224 (2012)
15. Sargolzaei, A., Yen, K.K., Abdelghani, M.: Time-delay switch attack on load frequency control in smart grid. Adv. Commun. Technol. **5**, 55–64 (2013)
16. Sargolzaei, A., Yen, K.K., Abdelghani, M.: Preventing time-delay switch attack on load frequency control in distributed power systems. IEEE Trans. Smart Grid **7**(2), 1176–1185 (2016)
17. Korkmaz, E., Dolgikh, A., Davis, M., Skormin, V.: Industrial control systems security testbed. In: 11th Annual Symposium on Information Assurance (ASIA 2016), pp. 13–18, June 2016
18. Rizzo, L.: Dummynet: a simple approach to the evaluation of network protocols. ACM SIGCOMM Comput. Commun. Rev. **27**(1), 31–41 (1997)
19. Carbone, M., Rizzo, L.: Dummynet revisited. ACM SIGCOMM Comput. Commun. Rev. **40**(2), 12–20 (2010)

20. Hu, J., Wang, Z., Gao, H., Stergioulas, L.K.: Robust sliding mode control for discrete stochastic systems with mixed time delays, randomly occurring uncertainties, and randomly occurring nonlinearities. IEEE Trans. Ind. Electron. **59**(7), 3008–3015 (2012)
21. Yang, R., Liu, G.-P., Shi, P., Thomas, C., Basin, M.V.: Predictive output feedback control for networked control systems. IEEE Trans. Ind. Electron. **61**(1), 512–520 (2014)
22. Skormin, V.: Introduction to Process Control. Springer, Cham (2016)
23. Dolgikh, A., Birnbaum, Z., Skormin, V.: Customized behavioral normalcy profiles for critical infrastructure protection. In: 8th Annual Symposium on Information Assurance (ASIA 2013), Albany, NY, pp. 15–22, June 2013
24. Liu, G.-P., Xia, Y., Chen, J., Rees, D., Hu, W.: Networked predictive control of systems with random network delays in both forward and feedback channels. IEEE Trans. Ind. Electron. **54**(3), 1282–1297 (2007)
25. Dunning, G.: Controllogix Programmable Automation Controllers with Labs Second Edition. Delmar Cengage Learning (2014)