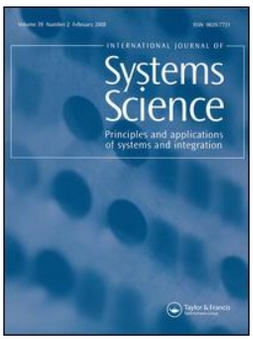

International Journal of Systems Science

ISSN: 0020-7721 (Print) 1464-5319 (Online) Journal homepage: https://www.tandfonline.com/loi/tsys20

Secure control of cyber physical systems subject to stochastic distributed DoS and deception attacks

Magdi S. Mahmoud, Mutaz M. Hamdan & Uthman A. Baroudi

To cite this article: Magdi S. Mahmoud, Mutaz M. Hamdan & Uthman A. Baroudi (2020): Secure control of cyber physical systems subject to stochastic distributed DoS and deception attacks, International Journal of Systems Science, DOI: 10.1080/00207721.2020.1772402

To link to this article: https://doi.org/10.1080/00207721.2020.1772402

Published online: 01 Jun 2020.

INTERNATIONAL JOURNAL OF SYSTEMS SCIENCE
https://doi.org/10.1080/00207721.2020.1772402

Secure control of cyber physical systems subject to stochastic distributed DoS and deception attacks

Magdi S. Mahmoud[a], Mutaz M. Hamdan[a] and Uthman A. Baroudi[b]

[a]Systems Engineering Department, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia; [b]Computer Engineering Department, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia

ABSTRACT

Cyber Physical Systems (CPS) such as power plants, water desalination utilities are just a few examples of systems that may come under stealth attacks. These attacks can threaten the proper operations of such systems without any indication. This problem necessitates the design of a control system that is able to work under such attacks. In this paper, an improved observer-based stabilising controller is proposed for CPS including random measurements and actuation delays and it is coming under distributed denial of service (DDoS) and deception attacks. The occurrences of DDoS and deception attacks are modelled as Bernoulli distributed white sequences with variable conditional probabilities. The criterion is presented in terms of linear matrix inequalities. Detailed simulation experiments on representative systems are shown to prove the applicability of the proposed methodology.

ARTICLE HISTORY
Received 23 April 2019
Accepted 17 May 2020

KEYWORDS
Cyber physical systems; distributed denial of service (DDoS) attack; deception attack; secure control system

1. Introduction

Cyber Physical Systems (CPS) are the integration of communication, computation and control for achieving the desired performance of physical systems. With its wide range of applications such as sustainable and blackout-free electricity generation and distribution, CPS attract the interest of researchers (Rajkumar et al., 2010). Other applications for CPS include clean and energy-aware buildings and cities, smart, medical and healthcare systems, transportation networks, chemical process control, smart grids, water/gas distribution networks, emergency management, etc. (Kim & Kumar, 2013).

CPS provide flexibility, reachability and profitability, yet, they become vulnerable to cyber attacks. Security issues increase the challenges of controlling CPS due to the fact these attacks are stealth and can affect the system behaviour without providing any notification about failure. These attacks can lead to a disruption to the physical system such as the coordination packets disarrangement in medium access control layers could be a result of injecting some malware by an adversary. Moreover, in order to destroy the normal operation, an attacker can illegally obtain access to the supervision centres while obtaining the encryption key. That means the system dynamics can be disturbed arbitrarily by the attacker, and when there is a lack of security protection either in hardware or software strategies he has the capability of inducing any perturbation (Ding et al., 2018).

The communication among the items of control systems, i.e. sensors, actuators and controllers, occurred through a common network medium. This network needs to be secured to prohibit vulnerability of attacking by adversaries during data transmission. These attacks could lead the system to instability or drive the plant to undesired operations as mentioned before. Thus considering of security issues is very important in designing of controllers for such a system.

From a control security viewpoint, Cyber attacks can be classified into two main types: (1) Denial of service (DoS) attacks, which are strategies used for occupying the communication resources in order to prohibit transmitting the measurement or control signals. (2) Deception attack, also called false data injection

CONTACT Magdi S. Mahmoud msmahmoud@kfupm.edu.sa Systems Engineering Department, King Fahd University of Petroleum and Minerals, P.O. Box 5067, Dhahran 31261, Saudi Arabia

(FDI) attacks, is defined as the modification of the data integrity for the transmitted packets among some cyber parts in the CPS.

The control of CPS under cyber attacks is one of the urgent and major issues in control engineering and it attracts a lot of research. Most of the existing works in the literature consider only one kind of the attacks such as Dolk et al. (2015), Dolk et al. (2017), Foroush and Martínez (2012), De Persis and Tesi (2014b), De Persis and Tesi (2014a), Yang et al. (2018) for the DoS attacks. And Amin et al. (2013), Ma et al. (2016), Huang and Dong (2017), Bai et al. (2017), Ding et al. (2017), Yuan and Xia (2017) for the deception attacks. Recently, Zhang et al. (2019) proposed a resilient state feedback controllers for a class of networked control systems affected by DoS attack, the closed-loop system is described as an aperiodic sampled-data system closely related to the bounds of duration time of the DoS attacks and a linear matrix inequality (LMI) based criterion is proposed to achieve the stability of the system. Ge et al. (2019) presented a two-stage distributed detection mechanism to alert the occurrence of distributed deception attack for a discrete time-varying system monitored by a sensor network. The security control problem in networked control systems (NCS) was discussed by Zhang et al. (2020), and further discussion on DoS (data available attacks) and data integrity attacks which include the deception attack was presented.

Some of the literature have considered two types of attacks, both of randomly occurred DoS and deception attacks were considered in designing an event-based security control system (Ding et al., 2016). In Yuan et al. (2017), the optimal control problem has been investigated for a class of networked control systems (NCSs) subject to DoS, deception and physical attacks using a delta operator approach and by applying ϵ-Nash equilibrium. A resilient linear quadratic Gaussian control strategy for NCSs affected by zero dynamic attacks was designed (Rhouma et al., 2018). Dynamic programming was applied for the control strategy and a power transmission strategy was designed using value iteration methods for a class of CPS subject to DoS attack (Yuan & Xia, 2018).

In comparison with single attack, considering two kinds of attack, i.e. DDoS attacks and deception attacks, is more practical since we do not know what the attacker decide to use in his attack. Technically, considering these two kinds of attacks require more discussion on the possible effects of each kind on the nominal system. In this paper, the effect of DDoS attacks is considered as variable delays in signal transmission among the CPS components. On the other hand, the effect of deception attacks is considered as modifying in the original signal as will be explained in Section 3. Considering these effects with several properties leads to complicate the problem under discussion and this we have succeed to solve in this paper. It is worth to note that all published works in the literature have assumed the attack to be random variable with a constant conditional probability, which does not fully represent practical situations. In our novel model, the attack is formulated and designed with variable conditional probabilities as will be described in Section 2.

It is worth to differentiate between *faults* and *deception* attacks. *Faults* are unintentional failures happen in a cyber physical system such as damaged pipe, faulty sensor and so on. On the other hand, *deception* attack is an intentional and planned modification to the cyber physical system data though compromising the CPS security. The differentiation between faults and deception or DoS attacks is not an easy task. The author in Yaseen and Bayart (2016) had proposed a methodology to distinguish faults and attacks despite.

Recently, Su et al. (2019) proposed an observer-based fault detection for switched system with all modes unstable. The average dwell time method and discretised Lyapunov function were implemented to obtain a switching signal and then exponential stability and H_∞ performance was achieved by solving linear matrix inequalities (LMIs). The existence of multiple time-varying delay and unknown nonlinear input fault was considered in designing a consensus observer based controller for multiagent systems (MAS) by Fattahi and Afshar (2019).

The most dangerous type of DoS attacks is the distributed DoS (DDoS) also called coordinated attack, in which a large number of compromised machines are used to perform the DoS attack (Hoque et al., 2017). Moreover, DDoS is frequently occurred due to the simplicity of creating it, low cost and its high impact on systems including the ability of completely disconnecting an organisation or causing a full collapse of the CPS (Ali et al., 2018; Semerci et al., 2018). It was shown that this attack could cause instability of power grids (Srikantha & Kundur, 2015) and produce long delay

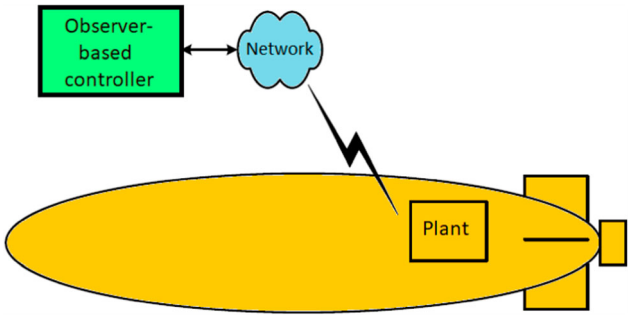

Figure 1. Diagrams of an example autonomous underwater vehicle CPS.

jitter on networked control systems (NCS) (Beitollahi & Deconinck, 2011).

Figure 1 shows a diagram of an example of CPS which consist of a plant (an autonomous underwater vehicle (AUV)), an observer-based controller, and a network. The plant (AUV) can include one or more actuators and/or sensors. The network can include a wired or wireless network such as a local area network (LAN), a wide area network (WAN), Wi-Fi, ethernet, cellular, the Internet or other suitable network. Actuators can include linear actuators, rotary actuators, electronically controlled valves, relays, etc. Sensors can include sensors generating one or more signals based on a measured location, speed, spatial orientation, temperature, pressure, actuator state, pH, weight, flow rate or other attribute. The observer-based controller can include a programmable logic controller or other suitable device. An autonomous underwater vehicle (AUV) will be described in detail and implemented as an example application to illustrate the effectiveness of our proposed method.

These critical consequences of DDoS motivate this work. We build up this novel model and formulate a novel problem observer-based controller of discrete time CPS affected by stochastic DDoS and cyber attacks in both forward (plant to controller) and backward (controller to actuator) signals. Following the summary of the main contributions of our work over previous literature:

(1) In our novel model, we work consider the coexistence of two types of cyber attacks: DDoS and deception attacks, in designing a secure observer-based stabilising controller for discrete-time CPS. Such scenario is realistic and has serious impact on cyber physical systems.
(2) In this novel design, we have tackled all possible scenarios of cyber attacks where both measurements and actuators signals are affected; meaning that in one hand, systems' sensors or transmitted signals have been modified by the attacker, delayed or both. On the other hand, the actuators' signals are also compromised by the attacks by altering its value, delaying, or both.
(3) The occurrences of DDoS and deception attacks are modelled as Bernoulli distributed white sequences with variable conditional probabilities. Such model resembles well a DDoS attack that employs several strategies initiated from several adversaries (Ali et al., 2018). This makes the proposed controller more suitable to practical applications. As far as the authors' knowledge, this is the first work, which considers random conditional probabilities, while other existing works considered constant conditional probabilities (see, e.g. Ding et al., 2016).
(4) A new controller is developed and analysed mathematically under the above conditions.
(5) The new controller is evaluated through an illustrative Autonomous underwater vehicle numerical example considering several scenarios of attacks to show the effectiveness of the proposed method.

The remaining of this paper is organised as follows. The problem of secure control of stochastic system subject to distributed DoS (DDoS) and deception attacks is formulated in Section 2. In Section 3, the theories to solve this problem is presented. An illustrative example is explained in Section 4 to show the effectiveness of the theorem. Finally, Section 5 concludes this work with our findings and future work.

2. Problem formulation and preliminaries

Industrial cyber physical systems (CPS) composed of plant, observer-based controller, and communication network is considered in this paper. Typical examples of such systems are SCADA systems, quadratic tank system and autonomous underwater vehicle (AUV), see e.g. Amin et al. (2013), Srikantha and Kundur (2015) and Ding et al. (2018). A system block diagram is shown in Figure 2. Nowadays, due to weak points between software and hardware components, CPS could be affected by several kinds of

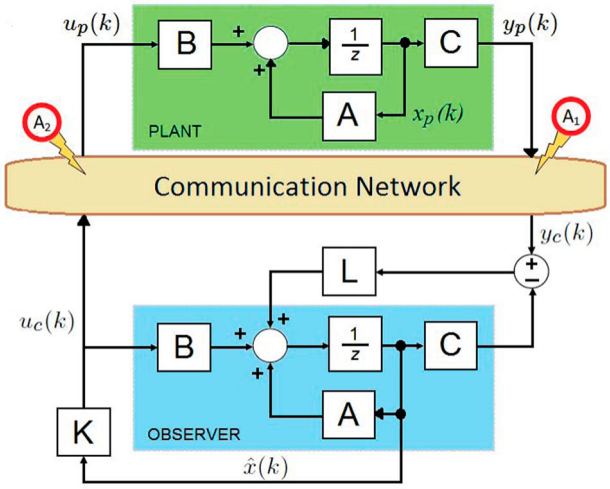

Figure 2. Attacks on cyber physical systems (CPS).

cyber attacks. In our novel model, we consider the occurrences of both DDoS and deception attacks in the forward communication (plant to observer) or backward communication (observer to plant) which are represented by (A_1) and (A_2) respectively in Figure 2.

The discrete-time linear time-invariant model of the plant is

$$x(k+1) = Ax(k) + Bu_p(k), \quad y_p(k) = Cx(k), \quad (1)$$

where $x(k) \in \Re^n$ is the plant's state vector and $u_p(k) \in \Re^m$ is the control input, and $y_p(k) \in \Re^p$ is the output vector. A, B and C are known matrices of the plant with appropriate dimensions. The measurement signal after passing the network is described by

$$y_c(k) = \alpha(k)[y_p(k) + \beta(k)(-y_p(k) + \zeta_y(k))] + (1 - \alpha(k))y_p(k - \tau_k^f), \quad (2)$$

where τ_k^f stands for *forward delay* with a Bernoulli distribution caused by DDoS attack in the forward path, and $\alpha(k)$ and $\beta(k)$ are Bernoulli distributed white sequences exhibiting the occurrence of forward DDoS and deception attacks, respectively, $\zeta_y(k)$ is the signal which affect the system in the forward deception attack.

Remark 2.1: In deriving (2), we follow the work of Ding et al. (2016) and Yuan et al. (2017) such that the denial of service attack is assumed to cause a delay in the signal, while the deception attack is assumed to replace the original signal by external signal $\vartheta(k)$. Also, assuming that the attacks' signals are energy-bounded is reasonable in engineering practice. So, it is valid to assume that the deception attack is norm-bounded (Yuan & Sun, 2015). Also, for the analysis convenience, the external signals sent by the attackers $\vartheta(k)$ could be rewritten as summation of two signals, i.e. $\vartheta(k) = (-y_p(k) + \zeta_y(k))$. Moreover, in this paper, the occurrences of DDoS and deception attacks are modelled as Bernoulli distributed white sequences with variable conditional probabilities $\alpha(k)$ and $\beta(k)$.

The observer-based controller below is implemented while considering an attack occurs on the forward path as shown in Figure 2:

$$\begin{aligned} &\textit{Observer}: \\ &\hat{x}(k+1) = A\hat{x}(k) + Bu_c(k) + L(y_c(k) - \hat{y}_c(k)) \\ &\hat{y}_c(k) = C\hat{x}(k) \\ &\textit{Controller}: \\ &u_c(k) = K\hat{x}(k) \\ &u_p(k) = \gamma(k)[u_c(k) + \delta(k)(-u_c(k) + \zeta_u(k))] \\ &\qquad + (1 - \gamma(k))u_c(k - \tau_k^b) \end{aligned} \quad (3)(4)$$

where $\hat{x}(k) \in \Re^n$ is the estimate of the states (1), $\hat{y}_c(k) \in \Re^p$ is the observer output, $L \in \Re^{n\times p}$ is the observer gain, $K \in \Re^{m\times n}$ is the controller gain and τ_k^b is the *backward delay* caused by the backward DDoS attack.

The stochastic variables $\gamma(k)$ and $\delta(k)$, mutually independent of $\alpha(k)$ and $\beta(k)$, are also a Bernoulli distributed white sequences exhibiting the occurrence of DDoS and deception backward attacks, respectively, $\zeta_u(k)$ is the signal which affect the system in the backward deception attack.

Here, we are assuming τ_k^b and τ_k^f to be bounded time-varying variables as follows:

$$\tau_f^- \le \tau_k^f \le \tau_f^+, \quad \tau_b^- \le \tau_k^b \le \tau_b^+ \quad (5)$$

Figure 3 shows different types of attacks affecting the system on forward and backward paths as well as the probability associated with each case. Here it is assumed that only one type of the attacks will happen, i.e. either DDoS attack ($j = 1, \ldots, 3$) or deception attack ($j = 4, \ldots, 7$) will take place at the same time.

The estimation error is defined as $e(k) = x(k) - \hat{x}(k)$. So, one can obtain

$$x(k+1) = Ax(k) + \gamma(k)(1 - \delta(k))BKx(k) + \gamma(k)\delta(k)B\zeta_u(k)$$

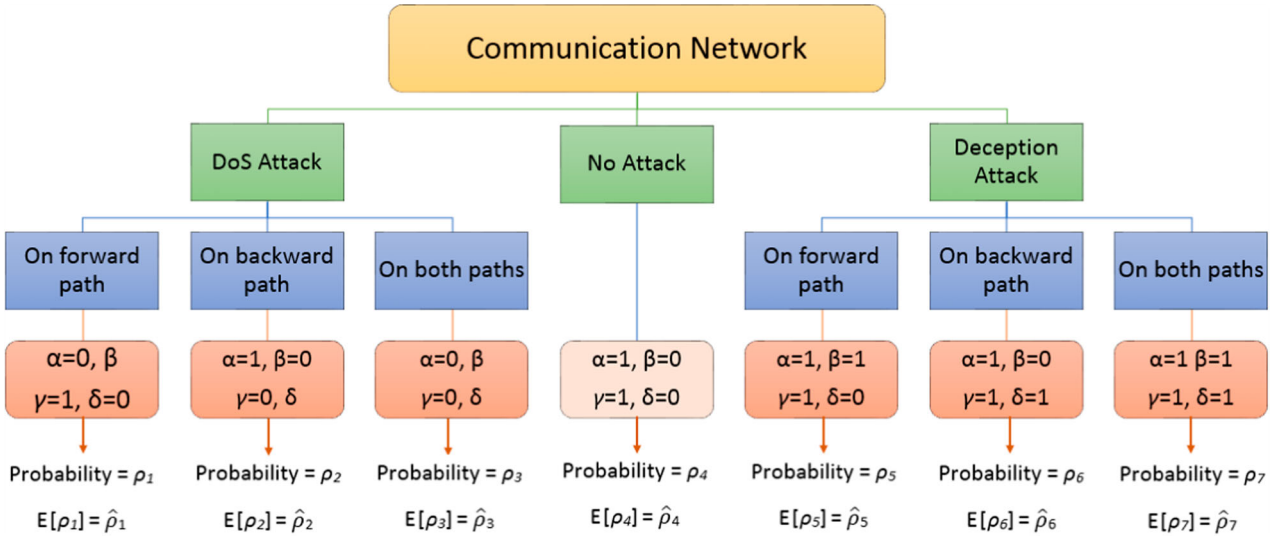

Figure 3. Types of the attack.

$$
\begin{aligned}
&+ (1-\gamma(k))BKx(k-\tau_k^b) \\
&- \gamma(k)(1-\delta(k))BKe(k) \\
&- (1-\gamma(k))BKe(k-\tau_k^b) \qquad (6)\\
e(k+1) = {}& (-BK+LC)x(k) + (A+BK-LC)e(k) \\
&+ \gamma(k)(1-\delta(k))BKx(k) \\
&+ \gamma(k)\delta(k)B\zeta_u(k) \\
&+ BK(1-\gamma(k))x(k-\tau_k^b) \\
&- \gamma(k)(1-\delta(k))BKe(k) \\
&- BK(1-\gamma(k))e(k-\tau_k^b) \\
&- \alpha(k)(1-\beta(k))LCx(k) \\
&- \alpha(k)\beta(k)L\zeta_y(k) \\
&- (1-\alpha(k))LCx(k-\tau_k^f) \qquad (7)
\end{aligned}
$$

By defining $\xi(k) = [x^{\mathrm{T}}(k) \quad e^{\mathrm{T}}(k)]^{\mathrm{T}}$, system (6) and (7) could be formulated as

$$
\begin{aligned}
\xi_j(k+1) = {}& \bar{A}_j\xi(k) + \bar{B}_j\xi(k-\tau_k^f) + \bar{C}_j\xi(k-\tau_k^b) \\
&+ \bar{D}_j\zeta(k), \quad j = 1,\ldots,7 \qquad (8)
\end{aligned}
$$

where $\zeta(k) = [\zeta_u^{\mathrm{T}}(k) \quad \zeta_y^{\mathrm{T}}(k)]^{\mathrm{T}}$, and $\{\bar{A}_j,\ \bar{B}_j,\ \bar{C}_j; \bar{D}_j,\ j = 1,\ldots,7\}$ and j is an index representing each situation in Figure (3) and their values as follows:

$$
\bar{A}_1 = \begin{bmatrix} A+BK & -BK \\ LC & A-LC \end{bmatrix},
$$

$$
\bar{A}_2 = \begin{bmatrix} A & 0 \\ -BK & A+BK-LC \end{bmatrix},
$$

$$
\bar{A}_3 = \begin{bmatrix} A & 0 \\ -BK+LC & A+BK-LC \end{bmatrix},
$$

$$
\bar{A}_4 = \begin{bmatrix} A+BK & -BK \\ 0 & A-LC \end{bmatrix},
$$

$$
\bar{A}_5 = \begin{bmatrix} A+BK & -BK \\ LC & A-LC \end{bmatrix},
$$

$$
\bar{A}_6 = \begin{bmatrix} A & 0 \\ -BK & A+BK-LC \end{bmatrix},
$$

$$
\bar{A}_7 = \begin{bmatrix} A & 0 \\ -BK+LC & A+BK-LC \end{bmatrix},
$$

$$
\bar{B}_1 = \bar{B}_3 = \begin{bmatrix} 0 & 0 \\ -LC & 0 \end{bmatrix}, \quad \bar{B}_j = \mathbf{0}, \quad j = 2,4,\ldots,7
$$

$$
\bar{C}_2 = \bar{C}_3 = \begin{bmatrix} BK & -BK \\ BK & -BK \end{bmatrix},
$$

$$
\bar{C}_j = \mathbf{0}, \quad j = 1,4,\ldots,7
$$

$$
\bar{D}_j = \mathbf{0}, \quad j = 1,\ldots,4, \quad \bar{D}_5 = \begin{bmatrix} 0 & 0 \\ 0 & -L \end{bmatrix},
$$

$$
\bar{D}_6 = \begin{bmatrix} B & 0 \\ B & 0 \end{bmatrix}, \quad \bar{D}_7 = \begin{bmatrix} B & 0 \\ B & -L \end{bmatrix} \qquad (9)
$$

Remark 2.2: The following can be noted from (9):

(1) When there is no attack or there is a DDoS attack, then

$$
\bar{A}_j + \bar{B}_j + \bar{C}_j = \begin{bmatrix} A+BK & -BK \\ 0 & A-LC \end{bmatrix}, \quad j = 1,\ldots,4 \qquad (10)
$$

The result of $\bar{A}_j + \bar{B}_j + \bar{C}_j, j = 1, \ldots, 4$ represents the fundamental matrix of system (8).

(2) Part of the fundamental matrix in (10) is changed due to signal injected by the attacker in the case of the deception attack.

Remark 2.3: The deception attack is considered as an arbitrary bounded energy signal with the following characteristic:

$$\zeta^{\mathrm{T}}\zeta < \eta^2 \tag{11}$$

The objective in this paper is to build an observer-based controller as formulated in (3) and (4) to guarantee the exponential stability in the mean square of the closed loop system (8). Our method is inspired by the switched time-delay systems (Mahmoud, 2010). For simplifying the expressions, we define each probability as ρ_j and expected value of it $\mathbb{E}[\rho_j]$ for $j = 1, \ldots, 7$ as shown in Figure 3.

3. Main results

The stability analysis and controller synthesis problems for the closed-loop system (8) will be investigated in this section. We will discuss the stability analysis problem to obtain a sufficient condition to guarantee the exponential stability in the mean square of system (8) with the given observer based controller (4) and (5). By expansion of the work of Mahmoud and Xia (2009), the main theorem will be established using the following candidate Lyapunov function:

$$V(\xi_j(k)) = \sum_{i=1}^{5} V_i(\xi_j(k)), \quad j = 1, \ldots, 7 \tag{12}$$

where

$$V_1(\xi_j(k)) = \sum_{j=1}^{7} \xi_j^{\mathrm{T}}(k) P \xi_j(k), \quad P > 0$$

$$V_2(\xi_j(k)) = \sum_{j=1}^{7} \sum_{i=k-\tau_k^f}^{k-1} \xi_j^{\mathrm{T}}(i) Q_j \xi_j(i), \quad Q_j = Q_j^{\mathrm{T}} > 0$$

$$V_3(\xi_j(k)) = \sum_{j=1}^{7} \sum_{i=k-\tau_k^b}^{k-1} \xi_j^{\mathrm{T}}(i) Q_j \xi_j(i)$$

$$V_4(\xi_j(k)) = \sum_{j=1}^{7} \sum_{\ell=-\tau_f^+ +2}^{-\tau_f^- +1} \sum_{i=k+\ell-1}^{k-1} \xi_j^{\mathrm{T}}(i) Q_j \xi_j(i)$$

$$V_5(\xi_j(k)) = \sum_{j=1}^{7} \sum_{\ell=-\tau_b^+ +2}^{-\tau_b^- +1} \sum_{i=k+\ell-1}^{k-1} \xi_j^{\mathrm{T}}(i) Q_j \xi_j(i) \tag{13}$$

Let us define real scalars $\upsilon > 0$ and $\varrho > 0$ with the following characteristics:

$$\upsilon \|\xi_j(k)\|^2 \le V(\xi_j(k)) \le \varrho \|\xi_j(k)\|^2, \quad j = 1, \ldots, 7 \tag{14}$$

Theorem 3.1: *For a given controller and observer gains K and L, system (8) is exponentially stable if there exist matrices $P > 0$, $Q_j^{\mathrm{T}} = Q_j > 0$, $j = 1, \ldots, 7$ and matrices F_i, U_i, and Z_i, $i = 1, 2$, satisfying the following LMI:*

$$\Upsilon_j = \begin{bmatrix} \Upsilon_{1j} & \Upsilon_{2j} & \Upsilon_{3j} \\ \bullet & \Upsilon_{4j} & \mathbf{0} \\ \bullet & \bullet & \Upsilon_{5j} \end{bmatrix} < 0 \tag{15}$$

$$\Upsilon_{1j} = \begin{bmatrix} \Psi_j + \Phi_{j1} & -F_1 + U_1^{\mathrm{T}} & -F_2 + U_2^{\mathrm{T}} \\ \bullet & -U_1 - U_1^{\mathrm{T}} - \hat{\rho}_j Q_j & 0 \\ \bullet & \bullet & -U_2 - U_2^{\mathrm{T}} - \hat{\rho}_j Q_j \end{bmatrix}$$

$$\Upsilon_{2j} = \begin{bmatrix} -F_1 + Z_1^{\mathrm{T}} - \Phi_{j2} & -F_2 + Z_2^{\mathrm{T}} - \Phi_{j3} \\ -U_1 - Z_1^{\mathrm{T}} & 0 \\ 0 & -U_2 - Z_2^{\mathrm{T}} \end{bmatrix},$$

$$\Upsilon_{3j} = \begin{bmatrix} \Phi_{j7} \\ 0 \\ 0 \end{bmatrix}$$

$$\Upsilon_{4j} = \begin{bmatrix} -Z_1 - Z_1^{\mathrm{T}} + \Phi_{j4} & \Phi_{j5} \\ \bullet & -Z_2 - Z_2^{\mathrm{T}} + \Phi_{j6} \end{bmatrix},$$

$$\Upsilon_{5j} = \Phi_{j8} - \eta I \tag{16}$$

where

$$\Psi_j = -P + \hat{\rho}_j(\tau_f^+ - \tau_f^- + \tau_b^+ - \tau_b^- + 2)Q_j + F_1 + F_1^{\mathrm{T}} + F_2 + F_2^{\mathrm{T}}$$

$$\Phi_{j1} = (\bar{A}_j + \bar{B}_j + \bar{C}_j)^{\mathrm{T}} \hat{\rho}_j P (\bar{A}_j + \bar{B}_j + \bar{C}_j)$$

$$\Phi_{j2} = (\bar{A}_j + \bar{B}_j + \bar{C}_j)^{\mathrm{T}} \hat{\rho}_j P \bar{B}_j,$$

$$\Phi_{j3} = (\bar{A}_j + \bar{B}_j + \bar{C}_j)^{\mathrm{T}} \hat{\rho}_j P \bar{C}_j$$

$$\Phi_{j4} = \bar{B}_j^{\mathrm{T}} \hat{\rho}_j P \bar{B}_j, \quad \Phi_{j5} = \bar{B}_j^{\mathrm{T}} P \bar{C}_j, \quad \Phi_{j6} = \bar{C}_j^{\mathrm{T}} \hat{\rho}_j P \bar{C}_j$$

$$\Phi_{j7} = (\bar{A}_j + \bar{B}_j + \bar{C}_j)^{\mathrm{T}} \hat{\rho}_j P \bar{D}_j, \quad \Phi_{j8} = \bar{D}^{\mathrm{T}} \hat{\rho}_j P \bar{D}_j$$

Proof: Let $y(k) = x(k+1) - x(k)$, so,

$$\xi_j(k - \tau_k^f) = \xi_j(k) - \sum_{i=k-\tau_k^f}^{k-1} y(i) \tag{17}$$

$$\xi_j(k-\tau_k^b) = \xi_j(k) - \sum_{i=k-\tau_k^b}^{k-1} y(i) \tag{18}$$

And system (8) can be represented as

$$\begin{aligned}\xi_j(k+1) = (\bar{A}_j + \bar{B}_j + \bar{C}_j)\xi_j(k) - \bar{B}_j\lambda(k) \\ - \bar{C}_j\epsilon(k) + \bar{D}_j\zeta(k)\end{aligned} \tag{19}$$

where

$$\lambda(k) = \sum_{i=k-\tau_k^f}^{k-1} y(i), \quad \epsilon(k) = \sum_{i=k-\tau_k^b}^{k-1} y(i).$$

Now, by evaluation of the difference of $V_1(\xi_j(k))$ along the solution of system (19), leads to

$$\begin{aligned}\mathbb{E}[\Delta V_1(\xi_j(k))] &= \mathbb{E}[V_1(\xi_j(k+1))] - V_1(\xi_j(k)) \\ &= \sum_{j=1}^{7}[\xi_j^{\mathrm{T}}(k)[\Phi_{j1} - P]\xi_j(k) \\ &\quad - 2\xi_j^{\mathrm{T}}(k)\Phi_{j2}\lambda(k) - 2\xi_j^{\mathrm{T}}(k)\Phi_{j3}\epsilon(k) \\ &\quad + \lambda^{\mathrm{T}}(k)\Phi_{j4}\lambda(k) + 2\lambda^{\mathrm{T}}(k)\Phi_{j5}\epsilon(k) \\ &\quad + \epsilon^{\mathrm{T}}(k)\Phi_{j6}\epsilon(k) + 2\xi_j^{\mathrm{T}}(k)\Phi_{j7}\zeta(k) \\ &\quad + \zeta^{\mathrm{T}}(k)(\Phi_{j8} - \eta I)\zeta(k)]\end{aligned} \tag{20}$$

A straightforward computation gives

$$\begin{aligned}&\mathbb{E}[\Delta V_2(\xi_j(k)] \\ &= \sum_{j=1}^{7}\hat{\rho}_j\left[\sum_{i=k+1-\tau_{k+1}^f}^{k}\xi_j^{\mathrm{T}}(i)Q_j\xi_j(i)\right. \\ &\quad \left. - \sum_{i=k-\tau_k^f}^{k-1}\xi_j^{\mathrm{T}}(i)Q_j\xi_j(i)\right] \\ &= \xi_j^{\mathrm{T}}(k)Q\xi_j(k) - \xi_j(k-\tau_k^f)Q_j\xi_j(k-\tau_k^f) \\ &\quad + \sum_{i=k+1-\tau_{k+1}^f}^{k-1}\xi_j^{\mathrm{T}}(i)Q_j\xi_j(i) \\ &\quad - \sum_{i=k+1-\tau_k^f}^{k-1}\xi_j(i)Q_j\xi_j(i)\end{aligned} \tag{21}$$

In view of

$$\sum_{i=k+1-\tau_{k+1}^f}^{k-1}\xi_j^{\mathrm{T}}(i)Q_j\xi_j(i)$$

$$\begin{aligned}&= \sum_{i=k+1-\tau_{k+1}^f}^{k-\tau_k^f}\xi_j^{\mathrm{T}}(i)Q_j\xi_j(i) + \sum_{i=k+1-\tau_k^f}^{k-1}\xi_j^{\mathrm{T}}(i)Q_j\xi_j(i) \\ &\le \sum_{i=k+1-\tau_k^f}^{k-1}\xi_j^{\mathrm{T}}(i)Q_j\xi_j(i) + \sum_{i=k+1-\tau_f^+}^{k-\tau_f^-}\xi_j^{\mathrm{T}}(i)Q_j\xi_j(i)\end{aligned} \tag{22}$$

We readily obtain

$$\begin{aligned}&\mathbb{E}[\Delta V_2(\xi_j(k))] \\ &\le \sum_{j=1}^{7}\hat{\rho}_j\left[\xi_j^{\mathrm{T}}(k)Q_j\xi_j(k) - \xi_j^{\mathrm{T}}(k-\tau_k^f)\right. \\ &\quad \left. \times\ Q_j\xi_j(k-\tau_k^f) + \sum_{i=k+1-\tau_f^+}^{k-\tau_f^-}\xi_j^{\mathrm{T}}(i)Q_j\xi_j(i)\right]\end{aligned} \tag{23}$$

By applying the same procedure, we have

$$\begin{aligned}&\mathbb{E}[\Delta V_3(\xi_j(k))] \\ &\le \sum_{j=1}^{7}\hat{\rho}_j\left[\xi_j^{\mathrm{T}}(k)Q_j\xi_j(k) - \xi_j^{\mathrm{T}}(k-\tau_k^b)\right. \\ &\quad \left. \times\ Q_j\xi_j(k-\tau_k^b) + \sum_{i=k+1-\tau_b^+}^{k-\tau_b^-}\xi_j^{\mathrm{T}}(i)Q_j\xi_j(i)\right]\end{aligned} \tag{24}$$

Finally

$$\begin{aligned}&\mathbb{E}[\Delta V_4(\xi_j(k))] \\ &= \sum_{j=1}^{7}\hat{\rho}_j\left[\sum_{\ell=-\tau_f^++2}^{-\tau_f^-+1}[\xi_j^{\mathrm{T}}(k)Q_j\xi_j(k) - \xi_j^{\mathrm{T}}(k+\ell-1)\right. \\ &\quad \left.\times\ Q_j\xi_j(k+\ell-1)]\right] \\ &= \sum_{j=1}^{7}\hat{\rho}_j\left[(\tau_f^+ - \tau_f^-)\xi_j^{\mathrm{T}}(k)Q_j\xi_j(k)\right. \\ &\quad \left. - \sum_{i=k+1-\tau_f^+}^{k-\tau_f^-}\xi_j^{\mathrm{T}}(i)Q_j\xi_j(i)\right]\end{aligned} \tag{25}$$

$$\mathbb{E}[\Delta V_5(\xi_j(k))]$$
$$= \sum_{j=1}^{7} \hat{\rho}_j \left[(\tau_b^+ - \tau_b^-)\xi_j^{\mathrm{T}}(k)Q_j\xi_j(k) - \sum_{i=k+1-\tau_b^+}^{k-\tau_b^-} \xi_j^{\mathrm{T}}(i)Q_j\xi_j(i) \right] \tag{26}$$

It follows from (17) and (18) that

$$\xi_j(k) - \xi_j(k-\tau_k^f) - \lambda(k) = 0 \tag{27}$$
$$\xi_j(k) - \xi_j(k-\tau_k^b) - \epsilon(k) = 0 \tag{28}$$

So, for any matrices F_i, U_i and Z_i, $i = 1, 2$, with appropriate dimensions, we could use the formulas:

$$2[\xi_j^{\mathrm{T}}(k)F_1 + \xi_j^{\mathrm{T}}(k-\tau_k^f)U_1 + \lambda^{\mathrm{T}}(k)Z_1] \times [\xi_j(k) - \xi_j(k-\tau_k^f) - \lambda(k)] = 0 \tag{29}$$
$$2[\xi_j^{\mathrm{T}}(k)F_2 + \xi_j^{\mathrm{T}}(k-\tau_k^b)U_2 + \epsilon^{\mathrm{T}}(k)Z_2] \times [\xi_j(k) - \xi_j(k-\tau_k^b) - \epsilon(k)] = 0 \tag{30}$$

The combination of (20)–(30) will lead to

$$\begin{aligned}
\mathbb{E}[\Delta V(\xi_j(k))] &\le \sum_{j=1}^{7} \Big[\xi_j^{\mathrm{T}}(k)\Psi_j\xi_j(k) \\
&+ \sum_{j=1}^{7} \xi_j^{\mathrm{T}}(k)(-2F_1 + 2U_1^{\mathrm{T}})\xi_j(k-\tau_k^f) \\
&+ \xi_j^{\mathrm{T}}(k)(-2F_2 + 2U_2^{\mathrm{T}})\xi_j(k-\tau_k^b) \\
&+ \xi_j^{\mathrm{T}}(k)(-2F_1 + 2Z_1^{\mathrm{T}} - 2\Phi_{j2})\lambda(k) \\
&+ \xi_j^{\mathrm{T}}(k)(-2F_2 + 2Z_2^{\mathrm{T}} - 2\Phi_{j3})\epsilon(k) \\
&+ \xi_j^{\mathrm{T}}(k-\tau_k^f)(-U_1 - U_1^{\mathrm{T}} - \hat{\rho}_j Q_j)\xi_j(k-\tau_k^m) \\
&+ \xi_j^{\mathrm{T}}(k-\tau_k^f)(-2U_1 - 2Z_1^{\mathrm{T}})\lambda(k) \\
&+ \xi_j^{\mathrm{T}}(k-\tau_k^b)(-U_2 - U_2^{\mathrm{T}} - \hat{\rho}_j Q_j)\xi_j(k-\tau_k^a) \\
&+ \xi_j^{\mathrm{T}}(k-\tau_k^b)(-2U_2 - 2Z_2^{\mathrm{T}})\epsilon(k) \\
&+ \lambda^{\mathrm{T}}(k)(-Z_1 - Z_1^{\mathrm{T}} + \Phi_{j4})\lambda(k) \\
&+ \epsilon^{\mathrm{T}}(k)(-Z_2 - Z_2^{\mathrm{T}} + \Phi_{j5})\epsilon(k) + \lambda^{\mathrm{T}}(k)\Phi_{j6}\epsilon(k) \\
&+ 2\xi_j^{\mathrm{T}}\Phi_{j7}\zeta + \zeta^{\mathrm{T}}(\Phi_{j8} - \eta I)\zeta \Big] \\
&= \sum_{j=1}^{7} \left[\Omega^{\mathrm{T}}(k)\widetilde{\Upsilon}_j\Omega(k) \right]
\end{aligned} \tag{31}$$

where

$$\Omega(k) = \left[\xi_j^{\mathrm{T}}(k) \quad \xi_j^{\mathrm{T}}(k-\tau_k^f) \quad \xi_j^{\mathrm{T}}(k-\tau_k^b) \quad \lambda^{\mathrm{T}}(k) \quad \epsilon^{\mathrm{T}}(k) \quad \zeta^{\mathrm{T}}(k)\right]^{\mathrm{T}} \tag{32}$$

and $\widetilde{\Upsilon}_j$ corresponds to Υ_j in (15) by Schur complements. If $\Upsilon_j < 0$, $j = 1, \ldots, 7$ holds, then

$$\begin{aligned}
\mathbb{E}[V(\xi_j(k+1)) - V(\xi_j(k))] &= \sum_{j=1}^{7} \left[\Omega^{\mathrm{T}}(k)\widetilde{\Upsilon}_j\Omega(k) \right] \\
&\le \sum_{j=1}^{7} \left[-\lambda_{\min}(\widetilde{\Upsilon}_j)\Omega^{\mathrm{T}}(k)\Omega(k) \right] \\
&< -\sum_{j=1}^{7} \left[\beta_j\Omega^{\mathrm{T}}(k)\Omega(k) \right]
\end{aligned} \tag{33}$$

where

$$0 < \beta_j < \min\left[\lambda_{\min}(\Upsilon_j), \max\{\lambda_{\max}(P),\ \lambda_{\max}(Q_j)\}\right]$$

Inequality (31) implies that $\mathbb{E}[V(\xi_j(k+1)) - V(\xi_j(k))] < -\phi V(\xi_j(k))$, $0 < \phi < 1$. In view of Yang et al. (2006), we have

$$||\xi_j(k)||^2 \le \frac{\upsilon}{\kappa}||\xi_j(0)||^2(1-\phi)^k + \frac{\lambda}{\upsilon\phi}$$

So, the exponential stability of system (8) can be verified. ■

Corollary 3.2: *For the case of DDoS attack only, for a given controller gain K and observer gain L. System* (8) *is exponentially stable if there exist matrices* $P > 0$, $Q_j^{\mathrm{T}} = Q_j > 0$, $j = 1, \ldots, 4$ *and matrices* F_i, U_i, *and* Z_i, $i = 1, 2$, *satisfying the following LMI:*

$$\Upsilon_j' = \begin{bmatrix} \Upsilon_{1j}' & \Upsilon_{2j}' \\ \bullet & \Upsilon_{3j}' \end{bmatrix} < 0 \tag{34}$$

$$\Upsilon_{1j}' = \begin{bmatrix} \Psi_j + \Phi_{j1} & -F_1 + U_1^{\mathrm{T}} & -F_2 + U_2^{\mathrm{T}} \\ \bullet & -U_1 - U_1^{\mathrm{T}} - \hat{\rho}_j Q_j & 0 \\ \bullet & \bullet & -U_2 - U_2^{\mathrm{T}} - \hat{\rho}_j Q_j \end{bmatrix}$$

$$\Upsilon'_{2j}=\begin{bmatrix}-F_1+Z_1^{\mathrm{T}}-\Phi_{j2} & -F_2+Z_2^{\mathrm{T}}-\Phi_{j3}\\ -U_1-Z_1^{\mathrm{T}} & 0\\ 0 & -U_2-Z_2^{\mathrm{T}}\end{bmatrix},$$

$$\Upsilon'_{3j}=\begin{bmatrix}-Z_1-Z_1^{\mathrm{T}}+\Phi_{j4} & \Phi_{j5}\\ \bullet & -Z_2-Z_2^{\mathrm{T}}+\Phi_{j6}\end{bmatrix}, \tag{35}$$

where

$$\begin{aligned}\Psi_j&=-P+\hat{\rho}_j(\tau_f^+-\tau_f^-+\tau_b^+-\tau_b^-+2)Q_j+F_1\\&\quad+F_1^{\mathrm{T}}+F_2+F_2^{\mathrm{T}}\\ \Phi_{j1}&=(\bar{A}_j+\bar{B}_j+\bar{C}_j)^{\mathrm{T}}\hat{\rho}_jP(\bar{A}_j+\bar{B}_j+\bar{C}_j),\\ \Phi_{j2}&=(\bar{A}_j+\bar{B}_j+\bar{C}_j)^{\mathrm{T}}\hat{\rho}_jP\bar{B}_j\\ \Phi_{j3}&=(\bar{A}_j+\bar{B}_j+\bar{C}_j)^{\mathrm{T}}\hat{\rho}_jP\bar{C}_j,\quad \Phi_{j4}=\bar{B}_j^{\mathrm{T}}\hat{\rho}_jP\bar{B}_j\\ \Phi_{j5}&=\bar{B}_j^{\mathrm{T}}P\bar{C}_j,\quad \Phi_{j6}=\bar{C}_j^{\mathrm{T}}\hat{\rho}_jP\bar{C}_j\end{aligned}$$

Proof: The proof of Corollary 3.2 could be obtained by applying the same procedure of the proof of Theorem 3.1. ■

Remark 3.1: Theorem 3.1 provides a stability condition for a class of CPS in the form of (8) with certain values of controller and observer gains subject to both DDoS and deception attacks. The DDoS attacks are considered to cause delays in transmitting signals from sensors to controller (forward bath) and\or from controller to actuators (backward path) with certain ranges, $[\tau_f^-,\tau_f^+]$, $[\tau_b^-,\tau_b^+]$, respectively. And the deception attacks could affect the forward and\or backward paths in the CPS with a signal bounded by η. On the other hand, Corollary 3.2 provides a similar stability condition for CPS with a similar circumstances but without deception attacks.

Theorem 3.3: *For a given delay bounds τ_f^+, τ_f^-, τ_b^+, τ_b^- and $\hat{\rho}_j$, $j=1,\ldots,7$. System (8) is exponentially stable if there exist matrices $X, Y_1, Y_2, \xi_j>0$, $j=1,\ldots,7$ and matrices H_i, M_i and R_i, $i=1,2$, satisfying the following LMI:*

$$\left[\begin{array}{ccc:c}\widehat{\Upsilon}_{1j} & \widehat{\Upsilon}_{2j} & \mathbf{0} & \\ \bullet & \widehat{\Upsilon}_{3j} & \mathbf{0} & \widehat{\Theta}_j\\ \bullet & \bullet & -\eta I & \\ \hdashline & \bullet & & -\hat{\rho}_j\widehat{X}\end{array}\right]<0 \tag{36}$$

where

$$\widehat{X}=\begin{bmatrix}X & 0\\ 0 & X\end{bmatrix}, \tag{37}$$

$$\begin{aligned}\widehat{\Psi}_j&=-\widehat{X}+\hat{\rho}_j(\tau_f^+-\tau_f^-+\tau_b^+-\tau_b^-+2)\xi_j\\&\quad+H_1+H_1^{\mathrm{T}}+H_2+H_2^{\mathrm{T}}\\ \widehat{\Upsilon}_{1j}&=\begin{bmatrix}\widehat{\Psi}_j & -H_1+M_1^{\mathrm{T}} & -H_2+M_2^{\mathrm{T}}\\ * & -M_1-M_1^{\mathrm{T}}-\hat{\rho}_j\xi_j & 0\\ * & * & -M_2-M_2^{\mathrm{T}}-\hat{\rho}_j\Xi_j\end{bmatrix}\\ \widehat{\Upsilon}_{2j}&=\begin{bmatrix}-H_1+R_1^{\mathrm{T}} & -H_2+R_2^{\mathrm{T}}\\ -M_1-R_1^{\mathrm{T}} & 0\\ 0 & -M_2-R_2^{\mathrm{T}}\end{bmatrix},\\ \widehat{\Upsilon}_{3j}&=\begin{bmatrix}-R_1-R_1^{\mathrm{T}} & 0\\ * & -R_2-R_2^{\mathrm{T}}\end{bmatrix}\\ \widehat{\Theta}_j&=[\widehat{\Theta}_{1j}\quad 0\quad 0\quad \widehat{\Theta}_{4j}\quad \widehat{\Theta}_{5j}\quad \widehat{\Theta}_{6j}]^{\mathrm{T}}\end{aligned} \tag{38}$$

with

$$\widehat{\Theta}_{1j}=\begin{bmatrix}XA^{\mathrm{T}}+Y_1^{\mathrm{T}}B^{\mathrm{T}} & 0\\ XA^{\mathrm{T}} & XA^{\mathrm{T}}-Y_2^{\mathrm{T}}\end{bmatrix},\quad j=1,\ldots,4,$$

$$\widehat{\Theta}_{15}=\begin{bmatrix}XA^{\mathrm{T}}+Y_1^{\mathrm{T}}B^{\mathrm{T}} & Y_2^{\mathrm{T}}\\ XA^{\mathrm{T}} & XA^{\mathrm{T}}\end{bmatrix},$$

$$\widehat{\Theta}_{16}=\begin{bmatrix}XA^{\mathrm{T}} & -Y_1^{\mathrm{T}}B^{\mathrm{T}}\\ XA^{\mathrm{T}} & XA^{\mathrm{T}}-Y_2^{\mathrm{T}}\end{bmatrix},$$

$$\widehat{\Theta}_{17}=\begin{bmatrix}XA^{\mathrm{T}} & -Y_1^{\mathrm{T}}B^{\mathrm{T}}+Y_2^{\mathrm{T}}\\ XA^{\mathrm{T}} & XA^{\mathrm{T}}\end{bmatrix}$$

$$\widehat{\Theta}_{4j}=\begin{bmatrix}0 & Y_2^T\\ 0 & Y_2^T\end{bmatrix},\quad j=1,3,$$

$$\widehat{\Theta}_{5j}=\begin{bmatrix}-Y_1^{\mathrm{T}}B^{\mathrm{T}} & -Y_1^{\mathrm{T}}B^{\mathrm{T}}\\ 0 & 0\end{bmatrix},\quad j=2,3$$

$$\widehat{\Theta}_{65}=\begin{bmatrix}0 & 0\\ 0 & -XL^{\mathrm{T}}\end{bmatrix},\quad \widehat{\Theta}_{66}=\begin{bmatrix}XB^{\mathrm{T}} & XB^{\mathrm{T}}\\ XB^{\mathrm{T}} & XB^{\mathrm{T}}\end{bmatrix},$$

$$\widehat{\Theta}_{67}=\begin{bmatrix}XB^{\mathrm{T}} & XB^{\mathrm{T}}\\ XB^{\mathrm{T}} & XB^{\mathrm{T}}-XL^{\mathrm{T}}\end{bmatrix},$$

$$\widehat{\Theta}_{4j}=0,\quad j=2,4,\ldots,7,$$

$$\widehat{\Theta}_{5j}=0,\quad j=1,4,\ldots,7,\quad \widehat{\Theta}_{6j}=0,\quad j=1,\ldots,4$$

and $K=Y_1X^{-1}$ and $L=Y_2X^{-1}C^{\dagger}$

Proof: By defining

$$\Theta_j=[(\bar{A}_j+\bar{B}_j+\bar{C}_j)\quad 0\quad 0\quad -\bar{B}_j\quad -\bar{C}_j\quad \bar{D}_j]^{\mathrm{T}}$$

We can describe matrix inequality (15) by

$$\Upsilon_j=\widetilde{\Upsilon}_j+\Theta_jP\Theta_j^{\mathrm{T}}<0 \tag{39}$$

$$\widetilde{\Upsilon}_j=\begin{bmatrix}\widetilde{\Upsilon}_{1j} & \widetilde{\Upsilon}_{2j} & \mathbf{0}\\ * & \widetilde{\Upsilon}_{3j} & \mathbf{0}\\ * & * & -\eta I\end{bmatrix}<0$$

$$\widetilde{\Upsilon}_{1j} = \begin{bmatrix} \Psi_j & -F_1 + U_1^{\mathrm{T}} & -F_2 + U_2^{\mathrm{T}} \\ * & -U_1 - U_1^{\mathrm{T}} - \hat{\rho}_j Q_j & 0 \\ * & * & -U_2 - U_2^{\mathrm{T}} - \hat{\rho}_j Q_j \end{bmatrix}$$

$$\widetilde{\Upsilon}_{2j} = \begin{bmatrix} -F_1 + Z_1^{\mathrm{T}} & -F_2 + Z_2^{\mathrm{T}} \\ -U_1 - Z_1^{\mathrm{T}} & 0 \\ 0 & -U_2 - Z_2^{\mathrm{T}} \end{bmatrix},$$

$$\widetilde{\Upsilon}_{3j} = \begin{bmatrix} -Z_1 - Z_1^{\mathrm{T}} & 0 \\ * & -Z_2 - Z_2^{\mathrm{T}} \end{bmatrix} \tag{40}$$

Select $\widehat{X} = P^{-1}$, and by applying Schur complements, we formulate matrix Υ_j in (39) as follows:

$$\left[\begin{array}{ccc:c} \widetilde{\Upsilon}_{1j} & \widetilde{\Upsilon}_{2j} & \mathbf{0} & \\ \bullet & \widetilde{\Upsilon}_{3j} & \mathbf{0} & \Theta_j \\ \bullet & \bullet & -\eta I & \\ \hdashline & \bullet & & -\hat{\rho}_j \widehat{X} \end{array}\right] < 0 \tag{41}$$

Multiplying the matrix inequality in (40) from right and left by $diag[\widehat{X}, \widehat{X}, \widehat{X}, \widehat{X}, \widehat{X}, I, I]$ and applying (37) and

$$\Xi_j = \widehat{X} Q_j \widehat{X}, \quad H_i = \widehat{X} F_i \widehat{X},$$
$$M_i = \widehat{X} U_i \widehat{X}, \quad R_i = \widehat{X} Z_i \widehat{X}, \quad j = 1, \ldots, 7, \quad i = 1, 2$$

Matrix inequality (36) subject (38) can be obtained. ■

Corollary 3.4: *For the case of DDoS attack only, for a given delay bounds τ_f^+, $\tau_f^-, \tau_b^+, \tau_b^-$ and $\hat{\rho}_j$, $j = 1, \ldots, 4$. Then, System* (8) *is exponentially stable if there exist matrices $0 < X$, Y_1, Y_2, $0 < \Xi_j$, $j = 1, \ldots, 4$ and matrices H_i, M_i and R_i, $i = 1, 2$, satisfying the following LMI:*

$$\left[\begin{array}{cc:c} \widehat{\Upsilon}'_{1j} & \widehat{\Upsilon}'_{2j} & \widehat{\Theta}_j \\ \bullet & \widehat{\Upsilon}'_{3j} & \\ \hdashline & \bullet & -\hat{\rho}_j \widehat{X} \end{array}\right] < 0 \tag{42}$$

$$\widehat{X} = \begin{bmatrix} X & 0 \\ 0 & X \end{bmatrix} \tag{43}$$

$$\widehat{\Psi}_j = -X + \hat{\rho}_j(\tau_f^+ - \tau_f^- + \tau_b^+ - \tau_b^- + 2)\Xi_j + H_1 + H_1^{\mathrm{T}} + H_2 + H_2^{\mathrm{T}}$$

$$\widehat{\Upsilon}'_{1j} = \begin{bmatrix} \widehat{\Psi}_j & -H_1 + M_1^{\mathrm{T}} & -H_2 + M_2^{\mathrm{T}} \\ * & -M_1 - M_1^{\mathrm{T}} - \hat{\rho}_j \Xi_j & 0 \\ * & * & -M_2 - M_2^{\mathrm{T}} - \hat{\rho}_j \Xi_j \end{bmatrix}$$

$$\widehat{\Upsilon}'_{2j} = \begin{bmatrix} -H_1 + R_1^{\mathrm{T}} & -H_2 + R_2^{\mathrm{T}} \\ -M_1 - R_1^{\mathrm{T}} & 0 \\ 0 & -M_2 - R_2^{\mathrm{T}} \end{bmatrix},$$

$$\widehat{\Upsilon}'_{3j} = \begin{bmatrix} -R_1 - R_1^{\mathrm{T}} & 0 \\ * & -R_2 - R_2^{\mathrm{T}} \end{bmatrix} \tag{44}$$

$$\widehat{\Theta}_j = \begin{bmatrix} \widehat{\Theta}_{1j} & 0 & 0 & \widehat{\Theta}_{4j} & \widehat{\Theta}_{5j} \end{bmatrix}^{\mathrm{T}}$$

$$\widehat{\Theta}_{1j} = \begin{bmatrix} XA^{\mathrm{T}} + Y_1^{\mathrm{T}} B^{\mathrm{T}} & 0 \\ XA^{\mathrm{T}} & XA^{\mathrm{T}} - Y_2^{\mathrm{T}} \end{bmatrix}, \quad j = 1, \ldots, 4$$

$$\widehat{\Theta}_{15} = \begin{bmatrix} XA^{\mathrm{T}} + Y_1^{\mathrm{T}} B^{\mathrm{T}} & Y_2^{\mathrm{T}} \\ XA^{\mathrm{T}} & XA^{\mathrm{T}} \end{bmatrix},$$

$$\widehat{\Theta}_{16} = \begin{bmatrix} XA^{\mathrm{T}} & -Y_1^{\mathrm{T}} B^{\mathrm{T}} \\ XA^{\mathrm{T}} & XA^{\mathrm{T}} - Y_2^{\mathrm{T}} \end{bmatrix}$$

$$\widehat{\Theta}_{4j} = \begin{bmatrix} 0 & Y_2^T \\ 0 & Y_2^T \end{bmatrix}, \quad j = 1, 3,$$

$$\widehat{\Theta}_{5j} = \begin{bmatrix} -Y_1^{\mathrm{T}} B^{\mathrm{T}} & -Y_1^{\mathrm{T}} B^{\mathrm{T}} \\ 0 & 0 \end{bmatrix}, \quad j = 2, 3$$

$$\widehat{\Theta}_{4j} = 0, \quad j = 2, 4, \ldots, 6,$$

$$\widehat{\Theta}_{5j} = 0, \quad j = 1, 4, \ldots, 6, \tag{45}$$

with $K = Y_1 X^{-1}$ and $L = Y_2 X^{-1} C^{\dagger}$.

Proof: The proof of Corollary 3.4 could be obtained by applying the same procedure of the proof of Theorem 3.3 with

$$\Theta_j = [(\bar{A}_j + \bar{B}_j + \bar{C}_j) \quad 0 \quad 0 \quad -\bar{B}_j \quad -\bar{C}_j]^{\mathrm{T}}$$

■

Remark 3.2: Theorem 3.3 offers a criterion to design stabilising observer-based feedback controller for a class of CPS in the form of (8) subject to both DDoS and deception attacks. The DDoS attacks are considered to cause delays in transmitting signals from sensors to controller (forward bath) and\or from controller to actuators (backward path) with certain ranges, $[\tau_f^-, \tau_f^+]$, $[\tau_b^-, \tau_b^+]$, respectively. And the deception attacks could affect the forward and\or backward paths in the CPS with a signal bounded by η. On the other hand, Corollary 3.4 provides a similar design method of an observer-based feedback controller for CPS with a similar circumstances but without deception attacks.

Remark 3.3: As noted in the above discussion, only the linear CPS are considered in this paper. However, all theorems and corollaries are applicable to the

following class of nonlinear CPS:

$$f(x(k)) = Ax(k) + Bu(k) + g(x, u) \tag{46}$$

where $g(x, u)$ is a bounded nonlinear function. Discussion of more general classes of nonlinear systems is left for future work.

4. Illustrative example

The effectiveness of the proposed method presented in this paper is shown by solving the control problem of the INFANTE Autonomous underwater vehicle (AUV) as per mentioned by Fadali and Visioli (2012) and Silvestre and Pascoal (2004). AUVs are robotic submarines that can be used for a variety of studies of the underwater environment. The vertical and horizontal dynamics of the vehicle must be controlled to remotely operate the AUV. The CPS of the AUV and the observer-based controller is shown in Figure 4. The forward attack A_1 and backward attack A_2 could be DDoS or deception attacks with probability as described in Figure 3

The simplified dynamics of the INFANTE AUV can be written in dimensional form as

- Surge motion equation:

$$m\dot{u} = C_X u^2 + C_{X_{vv}} v^2 + C_{X_{rr}} r^2 u^2 C_{X_{\delta_r \delta_r}} \delta_r^2 + C_{X_{\dot{u}}} \dot{u} + T$$

- Sway motion equation:

$$m\dot{v} + mur = C_{Y_r} ur + C_{Y_v} uv + C_{Y_{rrr}} r^3 C_{Yr|r|} r|r| + C_{Y_{v|v|}} v|v| + C_{Y_{\dot{v}}} \dot{v} C_{Y_{\dot{r}}} \dot{r} + C_{u^2} Y_{\delta_r} \delta_r$$

- Yaw motion equation:

$$\begin{aligned} I_z \dot{r} &= C_{N_v} uv + C_{N_{v|v|}} v|v| + C_{N_r} ur + C_{N_{r|r|}} r|r| \\ &\quad + C_{N_{rrr}} r^3 + u^2 C_{N_{\delta_r}} \delta_r \\ &\quad + C_{N_{\dot{v}}} \dot{v} + C_{N_{\dot{r}}} \dot{r}; \\ \dot{\psi} &= r; \end{aligned}$$

where u and v denote surge and sway speeds, ψ and r denote yaw and yaw rate, respectively. The symbol δ_r represents the rudder deflection and all other variables and parameters are defined by Silvestre

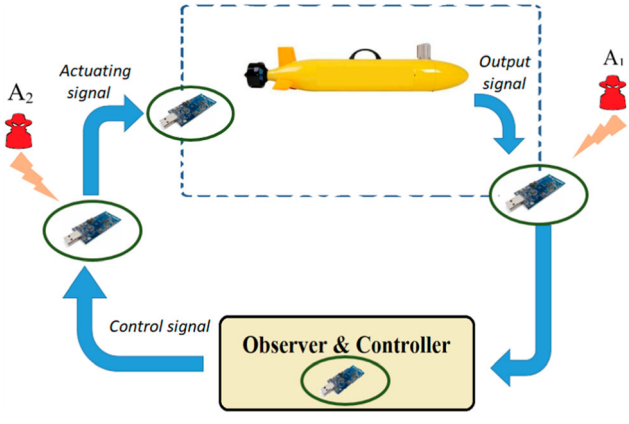

Figure 4. Schematic diagram of autonomous underwater vehicle CPS.

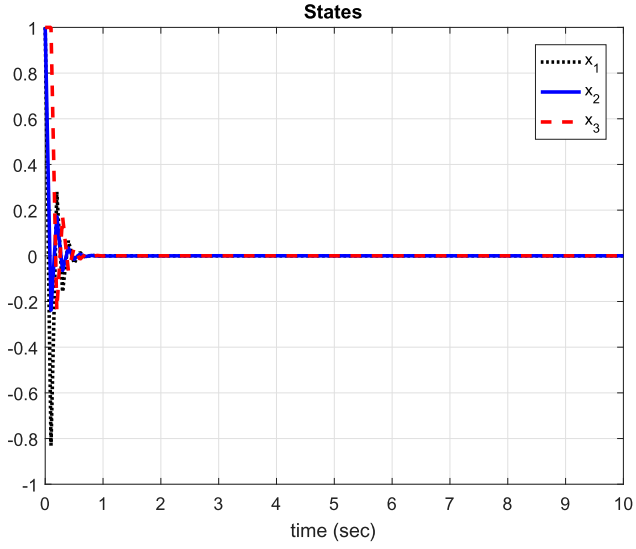

Figure 5. States with no attack.

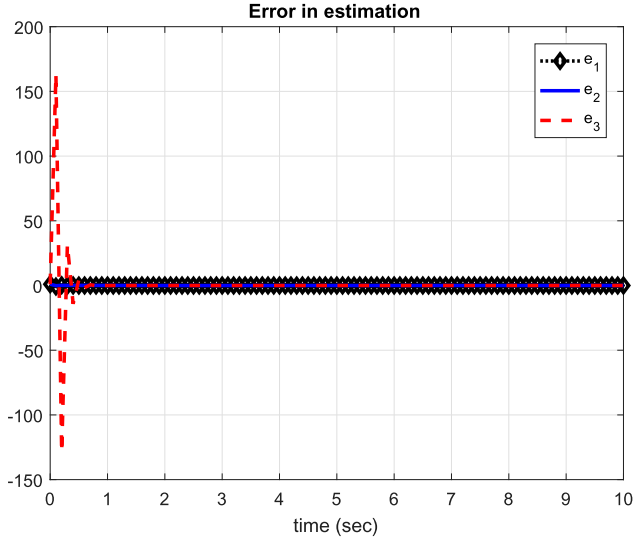

Figure 6. Error in estimation of states with no attack.

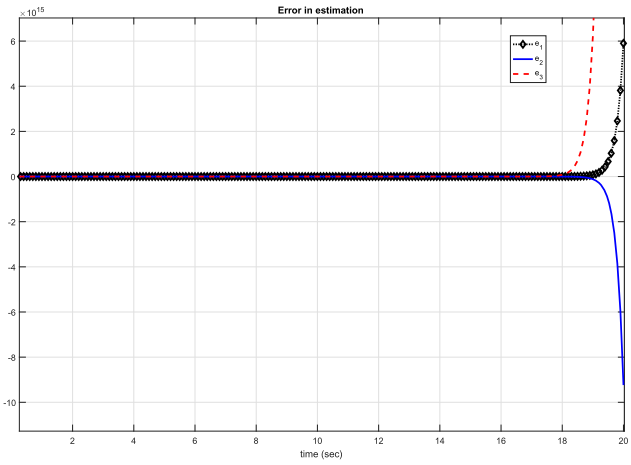

Figure 7. Error in estimation of states subject to cyber attacks with normal estimator.

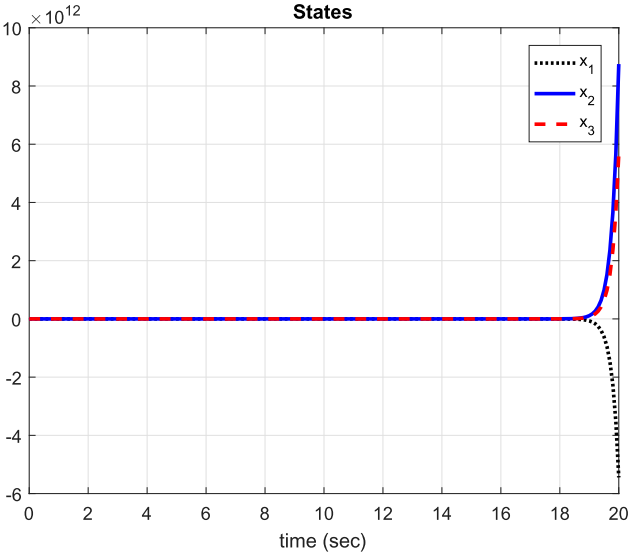

Figure 8. States of the AUV subject to cyber attacks with normal controller.

and Pascoal (2004). The objective of the controller is to guarantee a stable prescribed motion of the AUV. The linearised discrete-time model of the AUV is given by

$$x(k+1) = Ax(k) + Bu(k), \quad y(k) = Cx(k)$$

where x_1 is the sway speed, x_2 is the yaw angle, x_3 is the yaw rate and u is the rudder deflection, with

$$A = \begin{bmatrix} -0.14 & -0.69 & 0 \\ -0.19 & -0.048 & 0 \\ 0 & 1 & 0 \end{bmatrix}; \quad B = \begin{bmatrix} 0.056 \\ -0.23 \\ 0 \end{bmatrix}$$

$$C = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$$

The initial states value are assumed to be $x_1(0) = x_2(0) = x_3(0) = 1$. In this example, we assume that

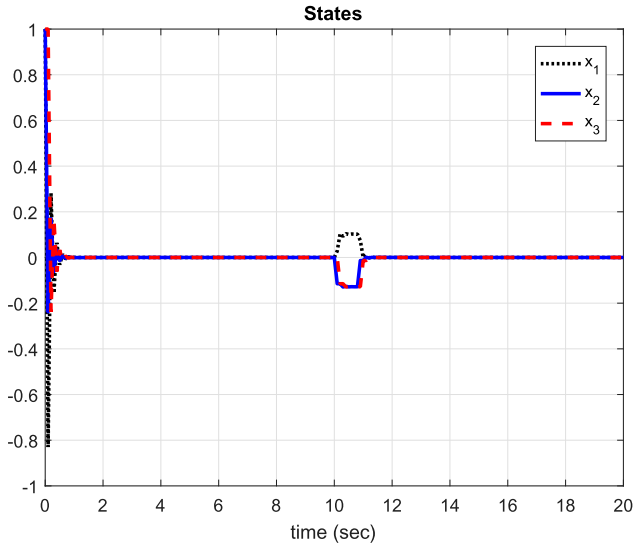

Figure 9. States with DDoS attack.

the probability of occurring an attack is 0.30, and the values of probability of the seven cases shown in Figure 3 are 0.06, 0.06, 0.03, 0.70, 0.06, 0.06, 0.03. Using YALMIP, the gains of the controller and estimator (3) and (4) were obtained to be as follows:

$$K = [0.00388 \quad 0.16755 \quad 0.00001]$$

$$L = [-0.038 \quad -0.076 \quad -162.02]^{\mathrm{T}}$$

Several scenarios were considered to verify the effectiveness of the proposed method and obtained result. In each scenario, both of the states and error in estimation for them were obtained and plotted using MATLAB/Simulink. The results are summarised as follows:

(1) System without attack, Figures 5–6.
Here the obtained gains of the observer and controller are applied on the AUV and system is simulated with free attack.

(2) System subject to attack but with normal controller, Figures 7 and 8.
These figures shows that if the nominal values of gains that obtained without considering the probability of occurring an attack are applied to the AUV while affected by an attack, the system will become unstable.

(3) System under DDoS attack, Figures 9 and 10.
The AUV is considered to be affected by DDoS attacks with variable probability in both forward and backward paths.

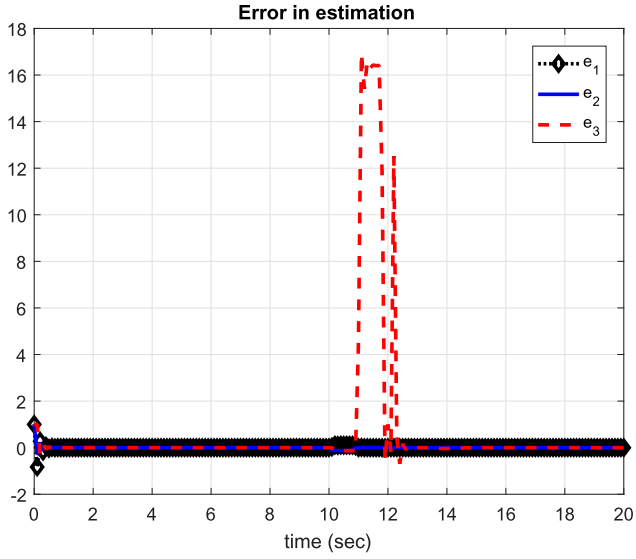

Figure 10. Error in estimation of states with DDoS attack.

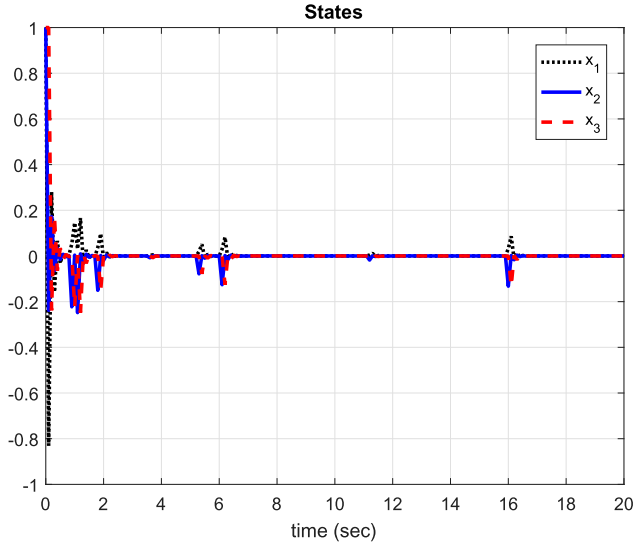

Figure 11. States with deception attack.

(4) System under Deception attack, Figures 11 and 12. The AUV is considered to be affected by deception attacks with variable probability in both forward and backward paths.

As shown in Figures 5–12, the designed observer-based controller shows stability in the system states and a small error in estimating these states under all possibilities of attacks. It can also be noted from Figures 6, 10 and 12 that there are few high peaks of error in estimation at certain times, while it is caused by the initial error in estimation in the first scenario and the occurrences of high value of attacks in the second and third scenarios, it does not affected the overall observer performance and the stability of the states.

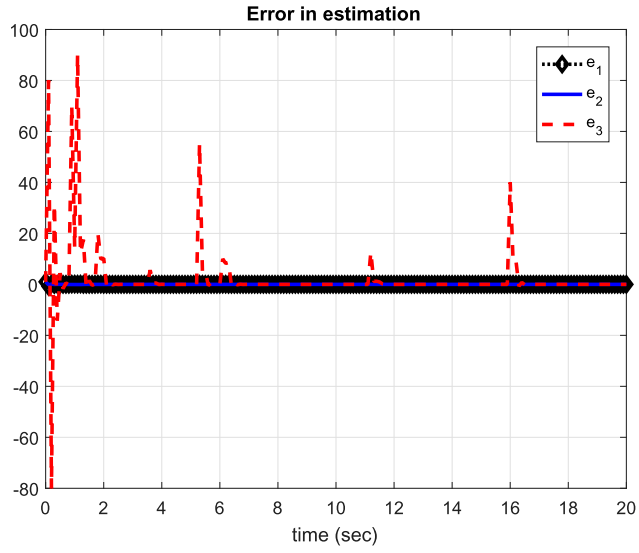

Figure 12. Error in estimation of states with deception attack.

5. Conclusion

In this paper, we proposed and studied an improved observer-based stabilising controller for CPS under distributed denial of service (DDoS) and deception attacks. The occurrences of DDoS and deception attacks are modelled as Bernoulli distributed white sequences with variable conditional probabilities. The criterion was formulated in terms of linear matrix inequalities. Detailed simulation experiments on representative systems have shown the applicability of the proposed methodology and its ability to keep the system within the desired stability conditions. As a future work, we are planning to test the proposed design using real prototype.

In this paper, we have considered linear CPS as described by (1) and also a class of nonlinear CPS as discussed in Remark 3.2. As a future work, this method could be extended more general nonlinear system. However, this requires modifying the observer and controller structures and upgrading the proposed method as well.

Acknowledgements

The authors acknowledge the support provided by the DSR at KFUPM through the distinguished professorship award project no. IN161965 and the support through the National Plan for Science, Technology and Innovation (MAARIFAH) – KACST

through the Science & Technology Unit at KFUPM, award project no. 15-ELE4117-04.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The authors acknowledge the support provided by the DSR at KFUPM through the distinguished professorship award project no. IN161965 and the support through the National Plan for Science, Technology and Innovation (MAARIFAH) – KACST through the Science & Technology Unit at KFUPM, award project no. 15-ELE4117-04.

Notes on contributors

Magdi S. Mahmoud obtained B.Sc. (Honors) in communication engineering, the M.Sc. in electronic engineering and the Ph.D. in systems engineering, all from Cairo University in 1968, 1972 and 1974, respectively. He has been a Professor of Engineering since 1984. He is now a Distinguished Professor at King Fahd University of Petroleum and Minerals (KFUPM), Saudi Arabia. He was on the faculty at different universities worldwide including Egypt (CU, AUC), Kuwait (KU), UAE (UAEU), UK (UMIST), USA (Pitt, Case Western), Singapore (Nanyang) and Australia (Adelaide). He lectured in Venezuela (Caracas), Germany (Hanover), UK ((Kent), USA (UoSA), Canada (Montreal) and China (BIT, Yanshan). He is the principal author of fifty-one (51) books, inclusive book-chapters and the author/co-author of more than 610 peer-reviewed papers. He is a fellow of the IEE, a senior member of the IEEE, the CEI (UK), and a registered consultant engineer of information engineering and systems (Egypt). He received the Science State Incentive Prize for outstanding research in engineering, (1978, 1986), the State Medal For Science And Art, First Class, (1978), and the State Distinction Award, (1986), Egypt. He awarded the Abdulhamed Showman Prize for Young Arab Scientists in the field of Engineering Sciences, (1986), Jordan. In 1992, he received the Distinguished Engineering Research Award, College of Engineering and Petroleum, Kuwait University, (1992), Kuwait. He is co-winner of the Most Cited Paper Award 2009, "Signal Processing", vol. 86, no. 1, 2006, pp. 140¡152. The Web of Science ISI selected his papers among the 40 best papers in *Electrical & Electronic Engineering* in July 2012. He interviewed for "People in Control", *IEEE Control Systems Magazine*, August 2010. He served as Guest Editor for the special issue "Neural Networks and Intelligence Systems in Neurocomputing" and Guest Editor for the *2015 International Symposium on Web of Things and Big Data* (WoTBD 2015) 18¡20 October 2015, Manama, Bahrain. He is a Regional Editor (Middle East and Africa) of International Journal of Systems, Control and Communications (JSCC), Inderscience Publishers since 2007, member of the Editorial Board of the *Journal of Numerical Algebra, Control and Optimization* (NACO), Australia since 2010, an Associate Editor of the *International Journal of Systems Dynamics Applications* (IJSDA), since 2011, member of the Editorial Board of the *Journal of Engineering Management*, USA since 2012 and an Academic Member of Athens Institute for Education and Research, Greece since 2015. Since 2016, He is an Editor of the *Journal Mathematical Problems in Engineering*, Hindawi Publishing Company, USA. He is currently actively engaged in teaching and research in the development of modern methodologies to distributed control and filtering, networked control systems, fault-tolerant systems, cyber-physical systems and information technology.

Mutaz M. Hamdan obtained Bachelor of Engineering degree (Honors) in Mechanical Engineering, Mechatronics Engineering Branch from Palestine Polytechnic University, Hebron, Palestine, in 2006. He received M. Sc. and Ph. D in Systems and Control Engineering from King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia, in 2012 and 2019. He has several published journal papers. He is currently a post-doctoral fellow at KFUPM, Saudi Arabia. His research interests include linear and nonlinear control systems, networked control systems, distributed control systems, and secure control systems.

Uthman A. Baroudi is currently an associate professor in the Department of Computer Engineering at KFUPM, Dhahran, Saudi Arabia. He received his B.Sc. and M.S. degrees from King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia in 1988 and 1990, respectively and in 2000, he received his Ph.D. from Concordia University, Montreal, Canada, all in Electrical Engineering. In 2000, he joined Nortel Networks, Ottawa, Canada, to work in R&D for next generation wireless networks. His research interests lie in the areas of cloud robotics networks, network design for IoT, cyber physical systems and security. Dr. Baroudi has over 100 publications in referred Journal and Conference Proceedings, and 34 US patents.

References

Ali, Y., Xia, Y., Ma, L., & Hammad, A. (2018). Secure design for cloud control system against distributed denial of service attack. *Control Theory and Technology*, *16*(1), 14–24. https://doi.org/10.1007/s11768-018-8002-8

Amin, S., Litrico, X., Sastry, S., & Bayen, A. M. (2013). Cyber security of water SCADA systems – Part I: Analysis and experimentation of stealthy deception attacks. *IEEE Transactions on Control Systems Technology*, *21*(5), 1963–1970. https://doi.org/10.1109/TCST.2012.2211873

Bai, C. Z., Pasqualetti, F., & Gupta, V. (2017). Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs. *Automatica*, *82*, 251–260. https://doi.org/10.1016/j.automatica.2017.04.047

Beitollahi, H., & Deconinck, G. (2011). A dependable architecture to mitigate distributed denial of service attacks

on network-based control systems. *International Journal of Critical Infrastructure Protection*, *4*(3–4), 107–123. https://doi.org/10.1016/j.ijcip.2011.06.003

De Persis, C., & Tesi, P. (2014a). *On resilient control of nonlinear systems under denial-of-service*. 53rd IEEE conference on decision and control, Los Angeles, CA, USA (pp. 5254–5259). https://doi.org/10.1109/CDC.2014.7040210

De Persis, C., & Tesi, P. (2014b). Resilient control under denial-of-service. *IFAC Proceedings Volumes*, *47*(3), 134–139. https://doi.org/10.3182/20140824-6-ZA-1003.02184

Ding, D., Han, Q. L., Xiang, Y., Ge, X., & Zhang, X. M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, *275*, 1674–1683. https://doi.org/10.1016/j.neucom.2017.10.009

Ding, D., Wang, Z., Wei, G., & Alsaadi, F. E. (2016). Event-based security control for discrete-time stochastic systems. *IET Control Theory & Applications*, *10*(15), 1808–1815. https://doi.org/10.1049/iet-cta.2016.0135

Ding, D., Wei, G., Zhang, S., Liu, Y., & Alsaadi, F. E. (2017). On scheduling of deception attacks for discrete-time networked systems equipped with attack detectors. *Neurocomputing*, *219*, 99–106. https://doi.org/10.1016/j.neucom.2016.09.009

Dolk, V., Tesi, P., De Persis, C., & Heemels, W. (2015). *Output-based event-triggered control systems under denial-of-service attacks*. 2015 54th IEEE conference on decision and control (CDC), Osaka, Japan (pp. 4824–4829). https://doi.org/10.1109/CDC.2015.7402972.

Dolk, V., Tesi, P., De Persis, C., & Heemels, W. (2017). Event-triggered control systems under denial-of-service attacks. *IEEE Transactions on Control of Network Systems*, *4*(1), 93–105. https://doi.org/10.1109/TCNS.2016.2613445

Fadali, M. S., & Visioli, A. (2012). *Digital control engineering: Analysis and design*. Academic Press.

Fattahi, M., & Afshar, A. (2019). Controller-based observer design for distributed consensus of multi-agent systems with fault and delay. *Journal of Control and Decision*, *6*(4), 217–235. https://doi.org/10.1080/23307706.2018.1458659

Foroush, H. S., & Martínez, S. (2012). *On event-triggered control of linear systems under periodic denial-of-service jamming attacks*. 2012 IEEE 51st IEEE conference on decision and control (CDC), Maui, HI, USA; pp. 2551–2556. doi:10.1109/CDC.2012.6425868.

Ge, X., Han, Q. L., Zhong, M., & Zhang, X. M. (2019). Distributed Krein space-based attack detection over sensor networks under deception attacks. *Automatica*, *109*, 108557. https://doi.org/10.1016/j.automatica.2019.108557

Hoque, N., Kashyap, H., & Bhattacharyya, D. (2017). Real-time DDoS attack detection using FPGA. *Computer Communications*, *110*, 48–58. https://doi.org/10.1016/j.comcom.2017.05.015

Huang, X., & Dong, J. (2017). *Adaptive optimization deception attack on remote state estimator of aero-engine*. 2017 29th Chinese control and decision conference (CCDC), Chongqing, China (pp. 5849–5854). https://doi.org/10.1109/CCDC.2017.7978214.

Kim, K. D., & Kumar, P. (2013). An overview and some challenges in cyber-physical systems. *Journal of the Indian Institute of Science*, *93*(3), 341–352.

Ma, L., Wang, Z., & Yuan, Y. (2016). *Consensus control for nonlinear multi-agent systems subject to deception attacks*. 2016 22nd international conference on automation and computing (ICAC), Colchester, UK (pp. 21–26). https://doi.org/10.1109/IConAC.2016.7604888.

Mahmoud, M. S. (2010). Switched time-delay systems. In Magdi S. Mahmoud (ed.), Switched time-delay systems (pp. 109–130). Springer. https://doi.org/10.1007/978-1-4419-6394-9_5

Mahmoud, M. S., & Xia, Y. (2009). Robust stability and stabilization of a class of nonlinear switched discrete-time systems with time-varying delays. *Journal of Optimization Theory and Applications*, *143*(2), 329–355. https://doi.org/10.1007/s10957-009-9560-1

Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010). *Cyber-physical systems: The next computing revolution*. Design automation conference, Anaheim, CA, USA (pp. 731–736). https://doi.org/10.1145/1837274.1837461

Rhouma, T., Chabir, K., & Abdelkrim, M. N. (2018). Resilient control for networked control systems subject to cyber/physical attacks. *International Journal of Automation and Computing*, *15*(3), 345–354. https://doi.org/10.1007/s11633-017-1059-x

Semerci, M., Cemgil, A. T., & Sankur, B. (2018). An intelligent cyber security system against DDoS attacks in SIP networks. *Computer Networks*, *136*, 137–154. https://doi.org/10.1016/j.comnet.2018.02.025

Silvestre, C., & Pascoal, A. (2004). Control of the INFANTE AUV using gain scheduled static output feedback. *Control Engineering Practice*, *12*(12), 1501–1509. https://doi.org/10.1016/j.conengprac.2004.02.012

Srikantha, P., & Kundur, D. (2015). *Denial of service attacks and mitigation for stability in cyber-enabled power grid*. 2015 IEEE power & energy society innovative smart grid technologies conference (ISGT), Washington, DC, USA (pp. 1–5). https://doi.org/10.1109/ISGT.2015.7131827

Su, Q., Fan, Z., & Li, J. (2019). Observer-based fault detection for switched systems with all unstable subsystems. *Journal of Control and Decision*, 1–14. https://doi.org/10.1080/23307706.2019.1651225

Yang, F., Wang, Z., Hung, Y., & Gani, M. (2006). H/sub/spl infin//control for networked systems with random communication delays. *IEEE Transactions on Automatic Control*, *51*(3), 511–518. https://doi.org/10.1109/TAC.2005.864207

Yang, C., Yang, W., & Shi, H. (2018). DoS attack in centralised sensor network against state estimation. *IET Control Theory & Applications*, *12*(9), 1244–1253. https://doi.org/10.1049/iet-cta.2017.0819

Yaseen, A. A., & Bayart, M. (2016). *Towards distinguishing between faults and cyber-attacks in the networked*

control system. 2016 world congress on industrial control systems security (WCICSS), London, UK (pp. 1–8). https://doi.org/10.1109/WCICSS.2016.7882611

Yuan, Y., & Sun, F. (2015). Data fusion-based resilient control system under DoS attacks: A game theoretic approach. *International Journal of Control, Automation and Systems*, *13*(3), 513–520. https://doi.org/10.1007/s12555-014-0316-9

Yuan, H., & Xia, Y. (2017). Secure filtering for stochastic nonlinear systems under multiple missing measurements and deception attacks. *IET Control Theory & Applications*, *12*(4), 515–523. https://doi.org/10.1049/iet-cta.2017.0868

Yuan, H., & Xia, Y. (2018). Resilient strategy design for cyber-physical system under DoS attack over a multi-channel framework. *Information Sciences*, *454–455*, 312–327. https://doi.org/10.1016/j.ins.2018.04.082

Yuan, Y., Zhang, P., Guo, L., & Yang, H. (2017). Towards quantifying the impact of randomly occurred attacks on a class of networked control systems. *Journal of the Franklin Institute*, *354*(12), 4966–4988. https://doi.org/10.1016/j.jfranklin.2017.05.016

Zhang, X., Han, Q., Ge, X., Ding, D., Ding, L., Yue, D., & Peng, C. (2020). Networked control systems: A survey of trends and techniques. *IEEE/CAA Journal of Automatica Sinica*, *7*(1), 1–17. https://doi.org/10.1109/JAS.6570654

Zhang, X., Han, Q., Ge, X., & Ding, L. (2019). Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks. *IEEE Transactions on Cybernetics*, 1–11. https://doi.org/10.1109/TCYB.2019.2956137