Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT

Faezeh Farivar, *Member, IEEE*, Mohammad Sayad Haghighi, *Senior Member, IEEE*, Alireza Jolfaei, *Senior Member, IEEE*, and Mamoun Alazab, *Senior Member, IEEE*

***Abstract*—This article proposes a hybrid intelligent-classic control approach for reconstruction and compensation of cyber attacks launched on inputs of nonlinear cyber-physical systems (CPS) and industrial Internet of Things systems, which work through shared communication networks. In this article, a class of *n*-order nonlinear systems is considered as a model of CPS while it is in presence of cyber attacks only in the forward channel. An intelligent-classic control system is developed to compensate cyber-attacks. Neural network (NN) is designed as an intelligent estimator for attack estimation and a classic nonlinear control system based on the variable structure control method is designed to compensate the effect of attacks and control the system performance in tracking applications. In the proposed strategy, nonlinear control theory is applied to guarantee the stability of the system when attacks happen. In this strategy, a Gaussian radial basis function NN is used for online estimation and reconstruction of cyber-attacks launched on the networked system. An adaptation law of the intelligent estimator is derived from a Lyapunov function. Simulation results demonstrate the validity and feasibility of the proposed strategy in car cruise control application as the testbed.**

***Index Terms*—Cyber physical system (CPS), intelligent estimator, Internet of Things (IoT), intrusion, neural network (NN), nonlinear control, security.**

Manuscript received August 1, 2019; revised October 8, 2019; accepted October 28, 2019. Date of publication November 28, 2019; date of current version January 17, 2020. This work was supported in part by the Institute for Research in Fundamental Sciences (IPM) under Grant CS1398-4-199. Paper no. TII-19-3577. *(Corresponding author: Faezeh Farivar.)*

F. Farivar is with the Department of Mechatronics and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran 1477893855, Iran, and also with the School of Computer Science, Institute for Research in Fundamental Sciences (IPM), Tehran 19395-5746, Iran (e-mail: F.Farivar@srbiau.ac.ir).

M. S. Haghighi is with the Department of Electrical and Computer Engineering, University of Tehran, Tehran 1439957131, Iran (e-mail: sayad@ut.ac.ir).

A. Jolfaei is with the Department of Computing, Macquarie University, Sydney, NSW 2109, Australia (e-mail: alireza.jolfaei@mq.edu.au).

M. Alazab is with the College of Engineering, IT & Environment, Charles Darwin University, Casuarina, NT 0810, Australia (e-mail: mamoun.alazab@cdu.edu.au).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2019.2956474

I. Introduction

CYBER-PHYSICAL systems (CPS) are the integration of computation, networking, and physical processes. A CPS consists of cooperating computational objects in connection with the physical world and its processes. CPSs have Internet of Things (IoT) as their close relative, yet keeping a distance from it due to the unique property of being associated with physical entities [1]–[3]. There are numerous CPS examples in autonomous cars, robotic surgery, intelligent buildings, smart electric grid, smart manufacturing, and implanted medical devices. A prominent property of CPSs is their pervasiveness and ubiquity, which are key enablers in the ubiquitous manufacturing technology. Pervasiveness is currently found in manufacturing in the context of industrial IoT [4]–[7] and service oriented architectures, to support intelligent control solutions.

Some CPSs rely on ad hoc networks or even the Internet to exchange messages and control signals among their components. This makes the system vulnerable to attacks launched in the network domain. Attacks on CPS could cause severe damage. This attack is not necessarily launched in the cyber world and may happen in the physical environment too. CPS is prone to attacks on all components. Therefore, information/cyber security techniques alone are not sufficient for guaranteeing the proper operation of CPS [8]. Control systems can be employed to complement the information security protection shields of CPS. Such systems can provide robustness to attacks. They can also be part of a more comprehensive intrusion detection and compensation system.

However, even cyber attacks in CPS may result in faults and failures in physical systems. One research challenge in such systems is to automatically compensate (deliberate) fault effects and to maintain the performance of the system at some acceptable level. The attacks or faults usually target sensors or system process. The aim of an attack detection and control system is to increase system availability through designing control algorithms that are capable of maintaining stability and performance in the presence of faults (CPS attacks). This article proposes an intelligent classic control approach for compensation of scalar attacks on nonlinear CPSs. It is assumed that the nonlinear CPS is experiencing cyber attacks in forward link. The designed control

system contains a nonlinear controller based on the variable structure (VS) method and a Gaussian Radial Basis Function Neural Network (GRBFNN) as an intelligent estimator for attack effect estimation. The VS control method is a robust control technique and involves two main steps, which are selecting an appropriate switching surface and establishing a robust control input. The GRBFNN estimator does online estimation of possible attacks and the adaptive neural VS controller is designed to compensate the effects of those attacks on the physical system and to control the performance for regulation and tracking aims. The adaptation law for the intelligent estimator is derived from a Lyapunov stability analysis. Thus, the system can be guaranteed to be asymptotically stable using this theorem.

The rest of this article is organized as follows. In Section II, a brief review of related papers is presented. In Section III, the control problem of a nonlinear CPS in presence of attack is formulated for a class of n-order nonlinear systems. In Section IV, the intelligent classic control strategy is designed and the stability proof is presented. Simulations results are discussed in Section V to show the effectiveness of the proposed strategy. Section VI concludes this article.

II. Related Work

There have been substantial efforts on CPS research in the last decade from different viewpoints such as applications, security, vulnerability, etc. Use of CPSs has expanded to various application areas such as energy, transportation, health, and manufacturing. A broad definition of CPS also includes Supervisory Control and Data Acquisition systems used in critical infrastructure such as intelligent transportation systems [9]–[11] and smart grid [12]. CPSs also embrace classic power networks, water networks, industrial control systems, and smart cars. In modern smart cars [13], [14], a network of small control systems is embedded to improve fuel efficiency, safety, and convenience. To analyze the vulnerabilities of CPSs, there are general approaches that can help investigate the effect of specific threats such as deception attacks [11], denial of service (DoS) [15], stealth attacks [16], reply attacks [17], covert attacks [18], false data injection attacks [19], [20], etc.

Another issue, which has gained considerable attention in recent years, is state estimation of linear systems when they are prone to faults, failures, or attacks. Observer-based strategies are commonly used as a basis for designing fault detection systems. The difference between the system output and output estimator is called the residue [21]. Residual generation approaches, using linear observers, have been widely used for fault detection. Among linear observers, Luenberger-like ones have severe limitations, due to their asymptotic performance and their sensitivity to (naturally bounded) modeling disturbances [22]. Robust sliding mode observers are designed for linear CPSs to detect state and sensor attacks and to estimate the attacks within a finite-time [23]. Also, attack estimation and compensation have been done for bounded modeling errors affecting the state equation of the US Western Electricity Coordinating Council (WECC) network power system [24].

Designing an appropriate control system is necessary to detect and, then, to safely run CPSs against cyber attacks. Estimation of attacks and performance control are fundamental to guaranteeing robustness and service continuity in these scenarios. There are many studies about fault detection, identification, and tolerant control [21] already. However, from the security perspective, there are fewer works on linear CPSs, e.g., for power networks [25], [26], water networks [27]–[29], etc.

Since sensor network and computer security have been applied as prevention mechanisms and they do not focus on how a control system can continue when the CPS under attack [30], two levels of defense are provided to have a safe operation of CPSF under attacks. First one is software security layers , which have been applied to prevent CPS from being attacked. It can provide security goals, integrity, availability, and confidently. The second level is to counteract/compensate the effect of attacks when the adversary/attacker penetrates to the CPS. It can be carried out by the control/compensator system. There are many studies on cyber attack detection [31]–[33], isolation, and the challenges on survivability of CPS [8], [17], [22]. According to our knowledge, there are few studies on the online reconstruction of attack. In [34], Nateghi *et al.* focused on the second level of defense against cyber-attacks, specifically, for the cyber-attack input reconstruction. In [23], a WECC network power system under attack was modeled as linear systems subject to unknown inputs altering the state attack and the sensor attack. Sliding mode observers are designed for both attack monitoring and reconstruction within a finite time. In [24], the extension of [23] is done. The attack compensation is carried out when the output tracks a given trajectory.

In [35], an intrusion detection and compensation framework was designed based on system identification to fight covert attacks. Errors of the output estimation are collected during the learning phase of system operation and, after that, the system behavior is monitored to see if it significantly deviates from the expected outputs. A compensating controller is also designed to intervene and replace the classic controller once the attack is detected.

In [36], an control approach is presented for tolerant control and compensation of cyber attacks occurred in inputs and outputs of a CPS of rotary gantry type. The malicious attacks are assumed to be of DoS kind and cause packet loss with high probability in the two signals: control input and output sensor. In the article, some classic and intelligent control strategies are studied in terms of robustness and effectiveness against cyber attacks.

Moreover, it is noticeable that most of studies are on linear dynamical systems. Hence, to study nonlinear dynamic systems, linearization approach based on Taylor series expansion is used. Many studies are focused on linear systems or linearized systems. Sometimes this simplification is not true.

In this article, we focus on nonlinear dynamic systems and there is no linear assumptions. Moreover, online estimation and compensation of the attacks plus external disturbances are investigated.

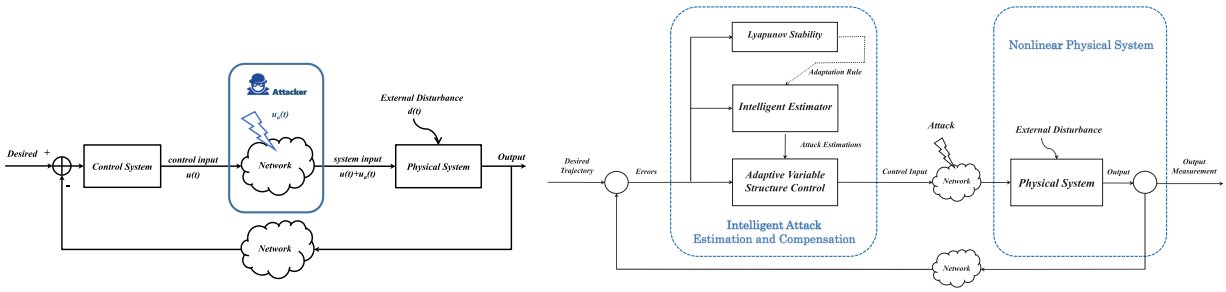

Fig. 1. (a) Intelligent attack estimation and compensation for a nonlinear physical system. (b) Nonlinear physical system is prone to cyber attack.

III. Control Problem Formulation for a Class of Nonlinear CPSs

In this article, the aim of the control system is to increase the safety and reliability of CPS under the assumption that it is vulnerable to attacks. This is achieved via designing control algorithms that are capable of maintaining stability and performance under attack scenarios.

Consider a class of n-order nonlinear CPSs that is described as standard (affine) nonlinear time invariant continuous-time system

$$\begin{aligned} x^{(n)}(t) &= f(x, \dot{x}, \ddot{x}, \ldots, x^{(n-1)}) + g(x, \dot{x}, \ddot{x}, \ldots, x^{(n-1)})u(t) \\ y(t) &= C[x, \dot{x}, \ddot{x}, \ldots, x^{(n-1)}]^T \end{aligned} \tag{1}$$

where f and g are known real continuous nonlinear functions of states, which are the dynamic functions of the CPS. $y \in \mathbb{R}$ is the output vector and $u \in \mathbb{R}$ is the control input of the CPS. It is assumed that the system is single-input single-output (SISO). The output matrix is denoted by C.

CPS input can be threatened by malicious attacks, which changes the control input by adding its value such as $u(t) + u_a(t)$, [see Fig. 1(a)]. Thus, (1) is changed as

$$\begin{aligned} x^{(n)}(t) &= f(x, \dot{x}, \ddot{x}, \ldots, x^{(n-1)}) \\ &\quad + g(x, \dot{x}, \ddot{x}, \ldots, x^{(n-1)})(u(t) + u_a(t)) \\ y(t) &= C[x, \dot{x}, \ddot{x}, \ldots, x^{(n-1)}]^T. \end{aligned} \tag{2}$$

Equation (2) can be written as

$$\begin{aligned} x^{(n)}(t) &= f(x, \dot{x}, \ddot{x}, \ldots, x^{(n-1)}) \\ &\quad + g(x, \dot{x}, \ddot{x}, \ldots, x^{(n-1)})u(t) + A(t) \\ y(t) &= C[x, \dot{x}, \ddot{x}, \ldots, x^{(n-1)}]^T \end{aligned} \tag{3}$$

where $A(t) = g(x, \dot{x}, \ddot{x}, \ldots, x^{(n-1)})u_a(t)$. We assume that the physical system is in presence of additive scalar disturbances affecting the states. Considering such possibility, (10) can be rewritten as

$$\begin{aligned} x^{(n)}(t) &= f(x, \dot{x}, \ldots, x^{(n-1)}) + g(x, \dot{x}, \ldots, x^{(n-1)})u(t) \\ &\quad + A(t) + d(t) \\ y(t) &= C[x, \dot{x}, \ddot{x}, \ldots, x^{(n-1)}]^T \end{aligned} \tag{4}$$

in which the term $A(t)$ models the attack corrupting the CPS directly. $d(t)$ represents any possible bounded external disturbance, $|d(t)| < \alpha$. Now, (4) can be rewritten as

$$\begin{aligned} \dot{x}_1(t) &= x_2(t) \\ \dot{x}_2(t) &= x_3(t) \\ &\vdots \\ \dot{x}_{n-1}(t) &= x_n(t) \\ \dot{x}_n(t) &= f(X) + g(X)u(t) + A(t) + d(t) \\ y(t) &= CX \end{aligned} \tag{5}$$

where $X = [x = x_1, \dot{x} = x_2, \ldots, x^{(n-1)} = x_n]^T$ is the CPS state vector. The CPS works under following assumptions.

1) The system is SISO. Hence, it is assumed that $C = [1, 0, \ldots, 0]^T$.
2) The mathematical model of the physical system is known.
3) The state vector is not available and only the output is available and measurable.
4) When we need to calculate the state vector, it can be obtained by using the measured output and the mathematical model of the physical system.
5) The feedback link is secure. Thus, the output measurements are reliable.
6) The cyber attacks only happen in the forward link and on the control input through disrupting the control signal by adding the attack vector, which is illustrated in Fig. 1(a).
7) The physical system works in presence of external disturbances, which affect the states.
8) There is no fault on the physical system and sensors.

Note that several types of attacks may threaten CPSs and they may affect either the physical or cyber components of the systems. In this article, deception and stealth attacks may affect the system, respectively. Deception attacks refer to the possibility of compromising the integrity of control packets or measurements and are carried out by altering the behavior of sensors and actuators [8]. In a stealth attack, the attacker modifies some sensors readings by physically tampering with the individual meters or by getting access to some communication channels [8].

In this article, model of the attack signal is described by

$$A(t) = \zeta(X, t) \tag{6}$$

in which X is the state vector and t is time. The function ζ is unknown yet bounded. Although the exact function is deemed to be unknown, we assume the attack function is predictable. Also, the bounds of the model functions (and also all their time derivatives) are known and available when we design the classic VS control system. $|\zeta(X,t)| < \beta_0$, $|\dot{\zeta}(X,t)| < \beta_1$, ..., $|\zeta^{(n)}(X,t)| < \beta_n$.

Generally, the mentioned bounds are unknown and we design the intelligent adaptive VS control system to estimate models of the attack signals. The control objective of CPS is to enforce the output to track a desired trajectory, y_d. In order to achieve the control objective, we have to define the control input such that it is able to control the output while the system works under cyber attack.

The control error is defined as follows:

$$e(t) = y_d(t) - y(t). \tag{7}$$

Therefore, error dynamics are presented as

$$\begin{aligned}
\dot{e}_1(t) &= e_2(t)\\
\dot{e}_2(t) &= e_3(t)\\
&\cdots\\
\dot{e}_{n-1}(t) &= e_n(t)\\
\dot{e}_n(t) &= y_d^{(n)} - f(X) - g(X)u(t)\\
&\quad - A(t) - d(t).
\end{aligned} \tag{8}$$

In order to achieve the control objective, it is necessary to design an appropriate control input in a way that for any initial conditions of the CPS, the control errors converge to zero, i.e., the resulting control error vector satisfies the below equation (obviously, in presence of attacks)

$$\lim_{t\to\infty} \|E(t)\| \to 0 \tag{9}$$

where $E(t) = [e_1(t), e_2(t), \ldots, e_n(t)]^T$ and $\|.\|$ is the Euclidean norm of a vector.

Equation (2) can be written as follows:

$$\begin{aligned}
x^{(n)}(t) &= f(x, \dot{x}, \ddot{x}, \ldots, x^{(n-1)})\\
&\quad + g(x, \dot{x}, \ddot{x}, \ldots, x^{(n-1)})u(t) + A(t)\\
y(t) &= C[x, \dot{x}, \ddot{x}, \ldots, x^{(n-1)}]^T.
\end{aligned} \tag{10}$$

IV. Adaptive Robust VS Control System for Cyber Attacks

In this section, first, we design the intelligent adaptive robust VS control system to solve the control problem formulated in the previous section. Adaptive VS control is a nonlinear control method commonly found in industrial systems [37]–[39]. Stability of the designed control system is proven during this section. Moreover, the adaptation law of the intelligent observer of attacks is presented.

A. VS Control

One of the robust nonlinear classic control techniques is VS control. There are two steps to design a VS control system: first, an appropriate switching surface is selected such that the motion on the switching manifold is stable. Then, a robust control law is designed that guarantees the switching manifold reaches zero even in presence of uncertainties and disturbances [40]. The switching surface is defined as follows:

$$S(t) = \left(\frac{d}{dt} + \lambda\right)^{n-1} e(t) \tag{11}$$

where λ is a real positive constant that governs the rate of convergence of the switching surface. The coefficients of (11) are the Newtonian expanded sentences. Thus, $S(t)$ can be rewritten as follows:

$$\begin{aligned}
S(t) &= \binom{n-1}{0} e^{(n-1)}(t) + \binom{n-1}{1} \lambda e^{(n-2)}(t)\\
&\quad + \binom{n-1}{2} \lambda^2 e^{(n-3)}(t) + \cdots + \binom{n-1}{n-3} \lambda^{n-3} \ddot{e}(t)\\
&\quad + \binom{n-1}{n-2} \lambda^{n-2} \dot{e}(t) + \binom{n-1}{n-1} \lambda^{n-1} e(t).
\end{aligned} \tag{12}$$

Now, by substituting (8), we have

$$\begin{aligned}
S(t) &= \binom{n-1}{0} e_n(t) + \binom{n-1}{1} \lambda e_{n-1}(t)\\
&\quad + \binom{n-1}{2} \lambda^2 e_{n-2}(t) + \cdots + \binom{n-1}{n-3} \lambda^{n-3} e_3(t)\\
&\quad + \binom{n-1}{n-2} \lambda^{n-2}\, e_2(t) + \binom{n-1}{n-1} \lambda^{n-1} e_1(t).
\end{aligned} \tag{13}$$

The derivative of the above equation is as follows:

$$\begin{aligned}
\dot{S}(t) &= y_d^{(n)} - f(X) - g(X)u(t) - A(t) - d(t)\\
&\quad + \binom{n-1}{1} \lambda e_{n-1}(t) + \binom{n-1}{2} \lambda^2 e_{n-2}(t) +\\
&\quad \ldots + \binom{n-1}{n-2} \lambda^{n-2} e_3(t) + \binom{n-1}{n-1} \lambda^{n-1} e_2(t).
\end{aligned} \tag{14}$$

The VS control law that guarantees the stability of closed-loop controlled system is designed as follows:

$$\begin{aligned}
u_{\text{vs}}(t) &= \frac{1}{g(X)}[k_v\ \text{sgn}(S) + y_d^{(n)} - f(X)\\
&\quad + \binom{n-1}{1} \lambda e_{n-1}(t) + \binom{n-1}{2} \lambda^2 e_{n-2}(t) +\\
&\quad \cdots + \binom{n-1}{n-2} \lambda^{n-2}\, e_3(t) + \binom{n-1}{n-1} \lambda^{n-1} e_2(t)]
\end{aligned} \tag{15}$$

where

$$k_v \geqslant \eta + \alpha + \beta_0. \tag{16}$$

Note that α and β_0 are the upper bounds of external disturbance and $A(t)$. It is assumed that $f(X)$ and $g(X)$ are known functions,

and disturbances are modeled by $d(t)$. Moreover, η is a constant positive scalar parameter and $g(X) \neq 0$. Notice that η should be chosen appropriately not only to have the quick time of the reaching switching motion, which provides an appropriate robustness against the system uncertainties but also to relieve the chattering. According to the Lyapunov stability theorem, trajectories of error dynamics will converge to the switching surface $S(t) = 0$ using the control input presented in (15). This can be proven by defining the Lyapunov function as below

$$V_{\text{vsc}}(t) = \frac{1}{2} S^2(t). \tag{17}$$

The derivative of (17) is as follows:

$$\dot{V}_{\text{vsc}}(t) = S(t)\, \dot{S}(t). \tag{18}$$

By substituting (14) into (18), we have

$$\begin{aligned} V_{\text{vsc}}(t) = S(t)(y_d^{(n)} - f(X) - g(X)u(t) - A(t) - d(t) \\ + \binom{n-1}{1} \lambda e_{n-1}(t) + \binom{n-1}{2} \lambda^2 e_{n-2}(t) + \cdots \\ + \binom{n-1}{n-2} \lambda^{n-2} e_3(t) + \binom{n-1}{n-1} \lambda^{n-1} e_2(t)). \end{aligned} \tag{19}$$

If the control law presented in (15) is substituted into (19), the derivative of the defined Lyapunov function is obtained as

$$\dot{V}_{\text{vsc}}(t) \leq -\eta \left| S(t) \right|. \tag{20}$$

Thus, the VS controller designed in (15) will asymptotically stabilize the error dynamics if the models of attack signals are known. As mentioned before, models of attack signals and their bounds are unknown. Thus, we develop the intelligent adaptive VS control system for detection of attacks in a way that the control system is able to compensate the effect of attacks on the CPS.

B. Intelligent Adaptive Neural Estimator

The GRBFNN is designed as an intelligent estimator to estimate the models of attack signals. However, $\hat{f}$ is usually given as

$$\hat{f} = w^T G(z, c, \sigma) \tag{21}$$

where $z = [z_1, z_2, \ldots, z_m]^T \in R^n$ is the input vector. $w = [w_1, w_2, \ldots, {w_m}^T]$ is the weighting vector of the output layer. The Gaussian radial basis function is represented by $G = [G_1, G_2, \ldots, {G_m}^T]$ in which $\sigma = [\sigma_1, \sigma_2, \ldots, \sigma_m]^T$ is the standard deviation and $c = [c_1, c_2, \ldots, {c_m}^T]$ is the mean vector of the Gaussian function. Note that the number of neurons is equal to m.

According to the universal approximation theorem, there exists an ideal neural network (NN) estimator f^* such that

$$f^*(t) = \hat{f}(t) + \epsilon = {w^*}^T G(z(t), c^*, \sigma^*) \tag{22}$$

where the approximation error is denoted by ϵ assumed to be bounded and w^*, c^*, σ^* are the optimal values, which lead to the best approximation of the nonlinear function f. Determination of these parameter values is difficult and challenging. Thus, the approximation function is presented as follows:

$$\hat{f}(t) = \hat{w}^T\, G(z(t), c, \sigma) \tag{23}$$

where $\hat{w}$ is the estimation value of the corresponding optimal parameter value. Note that the optimal parameter values are not unique. In this article, we focus on adjusting the weighting vectors and the standard deviation and mean vectors of Gaussian functions will not be trained. Thus, we define the error between the optimal and estimation weighting vectors as follows:

$$\tilde{w} = w^* - \hat{w}. \tag{24}$$

In this article, a GRBFNNs is applied to estimate the models of the input attack as follows:

$$\hat{f}_a(t) = \hat{w}_a^T\, G(z(t), c, \sigma). \tag{25}$$

Therefore

$$\tilde{w}_a = w_a^* - \hat{w}_a. \tag{26}$$

C. Intelligent Adaptive Robust VS Control

As mentioned before, the dynamic function of the attack, $A(t)$ is unknown, but it is assumed to be predictable. Therefore, the classic VS controller designed in Section IV-A cannot be precisely obtained. Accordingly, a GRBFNN is used for approximation of the attack function. The structure of the GRBFNN estimator is described in the previous section. In this section, intelligent adaptive robust VS control is proposed to solve the mentioned problem.

The proposed scheme for detection and compensation of the malicious attack in nonlinear CPSs using intelligent VS control system is demonstrated in Fig. 1(b).

Theorem: Consider the control problem presented in (8). If the control law of the intelligent VS control system is appropriately designed as follows:

$$\begin{aligned} u(t) = \frac{1}{g(X)} [k\ \text{sgn}(S(t)) + y_d^{(n)} - f(X) - \hat{A}_d(t) \\ + \binom{n-1}{1} \lambda e_{n-1}(t) + \binom{n-1}{2} \lambda^2 e_{n-2}(t) \\ + \cdots + \binom{n-1}{n-2} \lambda^{n-2}\, e_3(t) + \binom{n-1}{n-1} \lambda^{n-1} e_2(t)] \end{aligned} \tag{27}$$

where $k \geqslant \eta + \alpha$, α is the upper bound of $d(t)$, and η is a constant positive scalar parameter and $g(X) \neq 0$, then, error trajectories will asymptotically converge to the switching surface $S(t) = 0$ and control error vector satisfies (9). Note that $\hat{A}_d(t)$ is the online estimation of the summation of $A(t)$ and $d(t)$. Note that $f(X)$ and $g(X)$ are known functions. The adaptation law of the intelligent online estimator is as follows:

$$\dot{\hat{w}_a} = -S(t) G_a(z(t), c, \sigma) \tag{28}$$

where $G_a(.)$ is the Gaussian radial basis function corresponding to the estimator of $A_d(t)$. $S(t)$ is the switching surface defined in (13). ◊

Proof: As mentioned before, the dynamic function of the attack, $A(t)$ is unknown, but it is assumed to be predictable. When its bounds $(\beta_0, \ldots, \beta_n)$ are known, there is no need to use the NNs for estimating the effect of attacks. We just apply our knowledge in the condition of the control law, as presented in (16). Here, there is no information about the boundaries of the attack function. Hence, we apply a GRBFNN to find online estimations of attack effects as depicted in Fig. 1(b). Accordingly, we define another the Lyapunov function for the proposed closed-loop system shown in Fig. 1(b) as follows:

$$V(t) = \frac{1}{2}S^2(t) + \frac{1}{2}\tilde{w}_a^T\tilde{w}_a. \tag{29}$$

The first derivative of this Lyapunov function is

$$\dot{V}(t) = S(t)\dot{S}(t) + \tilde{w}_a^T\dot{\tilde{w}}_a. \tag{30}$$

By substituting (26), it can be rewritten as follows:

$$\dot{V}(t) = S(t)\dot{S}(t) - \tilde{w}_a^T\dot{\hat{w}}_a. \tag{31}$$

By substituting (14), we have

$$\begin{aligned}\dot{V}(t) = S(t)[&y_d^{(n)} - f(X) - g(X)u(t)\\ &- A(t) - d(t) + \binom{n-1}{1}\lambda e_{n-1}(t)\\ &+ \binom{n-1}{2}\lambda^2 e_{n-2}(t) + \cdots +\\ &+ \binom{n-1}{n-3}\lambda^{n-3}e_4(t) + \binom{n-1}{n-2}\lambda^{n-2}e_3(t)\\ &+ \binom{n-1}{n-1}\lambda^{n-1}e_2(t)] - \tilde{w}_a^T\dot{\hat{w}}_a.\end{aligned} \tag{32}$$

If the control input is designed as (27), then (32) can be presented as

$$\begin{aligned}\dot{V}(t) \leqslant S(t)[&-k\ \mathrm{sgn}(s) + \hat{A}_d(t)\\ &- A(t) - d(t)] - \tilde{w}_a^T\dot{\hat{w}}_a.\end{aligned} \tag{33}$$

It can be simplified as

$$\dot{V}(t) \leqslant -k\,|S(t)| - S(t)[\underbrace{A(t) + d(t)} - \hat{A}_d(t)] - \tilde{w}_a^T\dot{\hat{w}}_a. \tag{34}$$

As presented in Section IV-B, there is an optimal approximation function achievable by a GRBFNN such that it can exactly approximate the summation of unknown functions as follows:

$$w^{*T}G(z(t), c, \sigma) = A(t) + d(t). \tag{35}$$

As mentioned before, $\hat{A}_d(t)$ is the online estimation of the summation of $A(t)$ and $d(t)$, then

$$\hat{w}_a^T\ G(z(t), c, \sigma) = \hat{A}_d(t). \tag{36}$$

To simplify (34), we have

$$\left[\underbrace{A(t) + d(t)} - \hat{A}_d(t)\right] = \hat{w}^{*T}G(z(t), c, \sigma) - \hat{w}_a^T\ G(z(t), c, \sigma). \tag{37}$$

As presented before, w^* is the optimal value of w. In this article, we only focus on adjusting w and other parameters (c and σ) are constant and not adjustable. Thus, (38) can be rewritten as follows:

$$\begin{aligned}\left[\underbrace{A(t) + d(t)} - \hat{A}_d(t)\right] &= (w^* - \hat{w}_a)^T\ G(z, c, \sigma\\ &= \tilde{w}_a^T G(z, c,\ \sigma).\end{aligned} \tag{38}$$

Thus, (34) is simplified as follows:

$$\dot{V}(t) \leqslant -k\,|S(t)| - S(t)\tilde{w}_a^T G(z, c, \sigma) - \tilde{w}_a^T\dot{\hat{w}}_a. \tag{39}$$

It can be simplified as

$$\dot{V}(t) \leqslant -k\,|S(t)| - \tilde{w}_a^T\left(S(t)G(z, c, \sigma) + \dot{\hat{w}}_a\right). \tag{40}$$

Let the adaptation law of the GRBFNN estimator be

$$\dot{\hat{w}}_a = -S(t)G(z, c, \sigma). \tag{41}$$

Substituting (41) into (40) will give

$$\dot{V}(t) \leqslant -k\,|S(t)|\,. \tag{42}$$

Therefore, the control input designed in (27) and the adaptation laws of the online estimator obtained in (28) will asymptotically stabilize the CPS against cyber attacks in the forward link. Tracking error dynamics will converge to zero. Moreover, weights of the GRBFNN estimator will converge to optimal values. □

Remark: The intelligent estimator works to do online estimation of the attack effects. According to the obtained adaptation law, its adaptation rule goes to zero when the switching surface converges to zero. It means that when the defined errors are zero, the learning of the intelligent estimator is stopped. Vice versa, when there are errors on the closed-loop system, the intelligent estimator starts to detect and estimate the disrupting effects caused by attacks or/and external disturbances. Note that the intelligent estimator can adapt itself after a short time from staring to learn, which depends on the learning rate of the designed GRBFNN.

V. Evaluation Results and Discussions

In this section, we evaluate the proposed method on a physical example, which is a heavy-duty vehicle.

A. Simulation Setup

The scheme of an heavy duty vehicle system (HDVS) is illustrated in Fig. 2. The vehicle dynamics can be modeled by applying Newton's second law as follows [41]:

$$ma = F_e - F_a - F_r - F_g \tag{43}$$

where F_e is the force produced by the engine, F_a is the force due to aerodynamic drag, F_r is the rolling resistance force on tires, and F_g is the gravitational force due to the mass of the vehicle when going up on a slope. Equation (43) can be rewritten by incorporating the mentioned forces as follows:

$$m_{\text{tot}}\dot{v}(t) = k_e T_e(t) + k_a v^2(t) + k_r\cos(\alpha(\varsigma)) + k_g\sin(\alpha(\varsigma)) \tag{44}$$

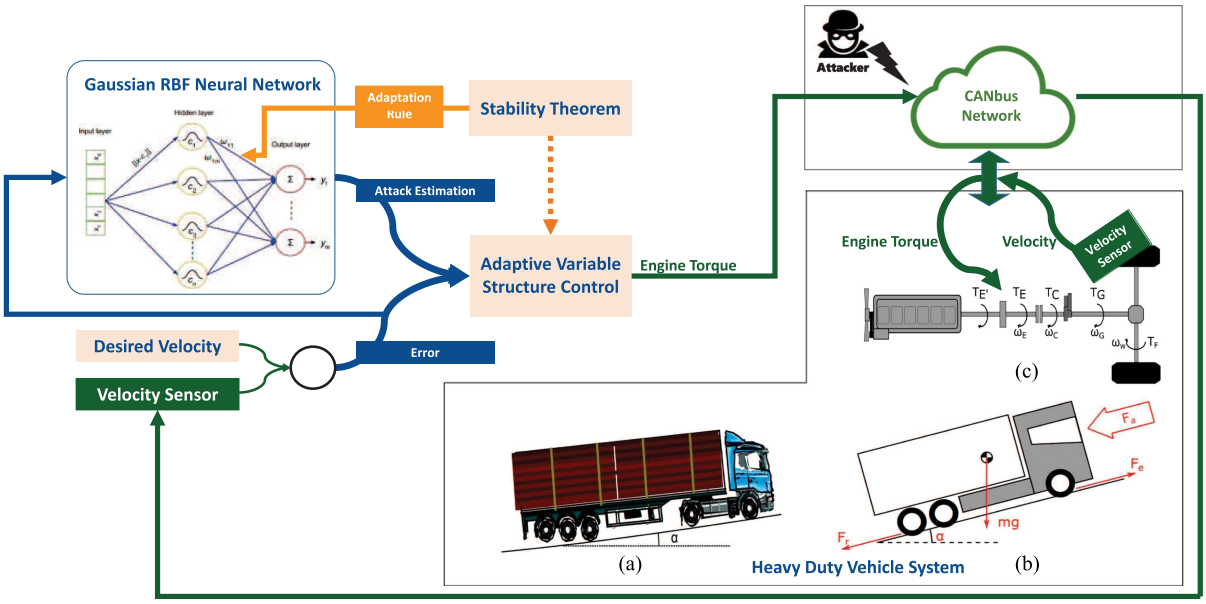

Fig. 2. Proposed control scheme for the HDV system when it is prone to cyber attacks. (a) Scheme of an HDV system where α is a road slope. (b) Forces acting on the vehicle when traveling on a road. (c) Simplified model of the HDV drivetrain. 1. Engine. 2. Flywheel. 3. Clutch. 4. Gearbox. 5. Final Drive. 6. Wheels [41].

where T_e is the engine torque with flywheel, v is the vehicle speed, $\alpha(\varsigma)$ is the road angle (which is a function of the position ς along the road), and the total mass is

$$m_{\text{tot}} = m + \frac{J_w}{r_w^2} + \frac{\gamma_G^2 \gamma_F^2 \eta_G \eta_F J_e}{r_w^2}. \tag{45}$$

The vehicle mass is denoted by m. The second term is related to the wheel inertia and the third term is related to the flywheel inertia. J_w is the rotational inertia of wheels and r_w is the wheel radius. γ_G and γ_F are the gearbox and final drive gear ratios. η_G and η_F are the gearbox and final drive efficiency coefficients. Other coefficients of (44) are as follows: $k_e = \frac{\gamma_G \gamma_F \eta_G \eta_F}{r_w}$, $k_a = \frac{1}{2} c_d A_a \rho_a$, $k_r = c_r mg$, $k_g = mg$, where c_d is the drag coefficient, A_a is the frontal area of the vehicle, ρ_a is the density of air, c_r is the rolling friction coefficient, and g is the gravitational constant. The HDV cruise control aim is to maintain the speed of the HDVS at a constant value (v_{cc}) under any possible attacks or external disturbances. The parameters used for simulations are available in [41] as follows: $v_{cc} = 80$ km/h, $c_d = 0.56$, $m = 40\,000$ kg, $A_d = 10\text{m}^2$, $\gamma_G = 1$, $\rho_d = 1.29$ kg/m^3, $\gamma_F = 2.71$, $c_r = 0.007$, $\eta_G = 0.97$, $g = 9.82$, $\eta_F = 0.97$, $J_w = 32.9$ kgm^2, $r_w = 0.5$ m, and $J_E = 3.5$ kgm^2.

As stated the system works in the presence of external disturbances and attacks. Therefore, (44) is represented as follows:

$$\begin{aligned} \dot{v}(t) &= \frac{1}{m_{\text{tot}}}(k_e T_e(t) + k_a v^2(t) + k_r \cos(\alpha(\varsigma)) \\ &\quad + k_g \sin(\alpha(\varsigma)) + A(t) + d(t)) \\ y(t) &= v(t) \end{aligned} \tag{46}$$

where T_e is the control input and v is the state variable. $A(t)$ presents the attack model. $d(t)$ is the external disturbance. Examples of the attacks as well as the external disturbance used in the simulations are depicted in Fig. 3(a) and (b). It is assumed that attacks and disturbance are bounded. The proposed control scheme of the HDV cruise system, which works under cyber attacks is depicted in Fig. 2. The control error is defined according to (7) as follows:

$$e(t) = v_{cc} - v(t). \tag{47}$$

Thus, according to (11), the switching surface is the same as the defined control error, i.e., (47). According to Theorem 1, the intelligent VS control input is designed as follows:

$$\begin{aligned} T_e(t) = \frac{m_{\text{tot}}}{k_e} \Bigg[& k\ \text{sgn}(S(t)) - \hat{A}(t) \\ & - \frac{k_a v^2 + k_r \cos(\alpha(\varsigma)) + k_g \sin(\alpha(\varsigma))}{m_{\text{tot}}} \Bigg] \end{aligned} \tag{48}$$

where $k \geqslant \eta + \alpha$, α is the upper bound of $d(t)$, and η is a positive constant scalar. Also, $\hat{A}_d(t)$ is the online estimation of the sum of $A(t)$ and $d(t)$. The adaptation rule of the intelligent online estimator is as follows:

$$\dot{\hat{w}}_a = -S(t) G_a(z(t), c, \sigma) \tag{49}$$

where $G_a(.)$ is the Gaussian radial basis function corresponding to the estimator of $A(t)$. $S(t)$ is the switching surface defined before. The pseudo code of the proposed control scheme with applying the GRBFNN for estimating attack function is presented in Algorithm 1. The parameter values of the designed controller are chosen as $\lambda = 1$, $k = 150$, and the number of neurons of the NN is $n = 5$. Note that the sign function of the control law is substituted by the saturation function to reduce chattering in the CPS system.

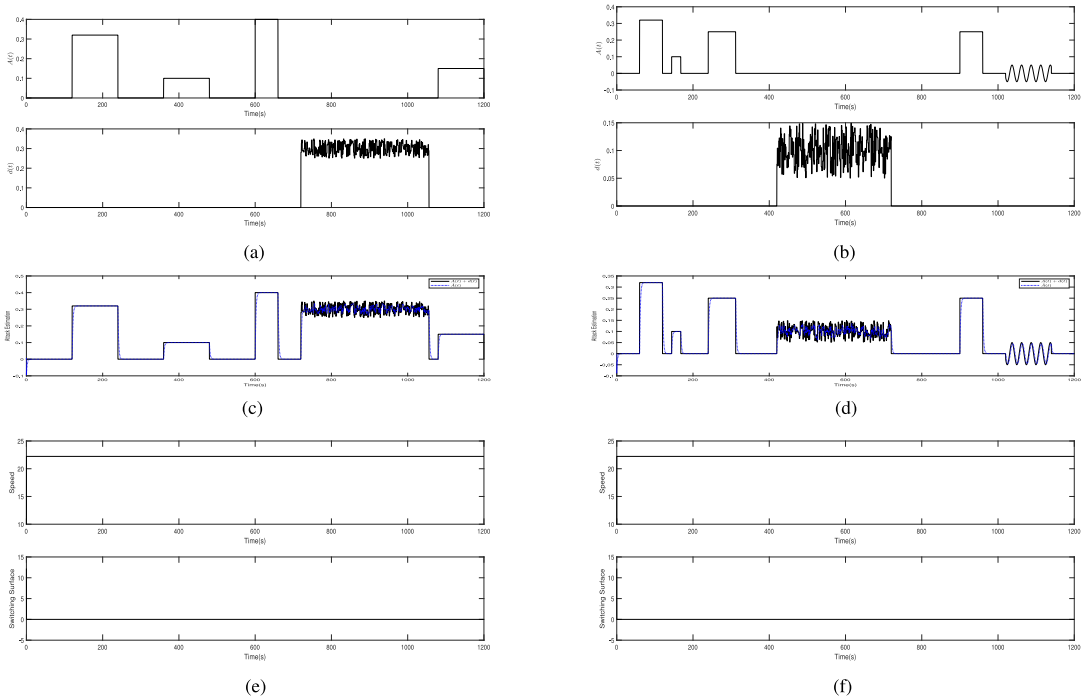

Fig. 3. [Example-The HDV system (Left Column: Case1 and Right Column: Case2)]. (a), (b) Occurred attacks and disturbances. (c), (d) Estimation of Attacks and Disturbance. (e), (f) Car Cruise Speed and Switching surface. (a) Case 1: Attacks and Disturbance. (b) Case 2: Attacks and Disturbance. (c) Case 1: Estimation of Attacks and Disturbance. (d) Case 2: Estimation of Attacks and Disturbance. (e) Case 1: Car Cruise Speed and Switching Surface. (f) Case 2: Car Cruise Speed and Switching Surface.

Algorithm 1: Algorithm of the Proposed Control Scheme for the HDV System (which works under cyber attacks).

Ensure: Control Objective

1: Create a desired set point for the velocity v_{cc}
2: Initialize the learning parameter of the Gaussian RBF Neural Network (GRBF-NN)
3: Upon receiving the HDV system velocity v through the shared CANbus network, do
4: Read v received through the shared CANbus network
5: Calculate the control error, E
6: Calculate the switching surface, S
7: Apply E to the GRBF-NN
8: Update the Learning parameter of the GRBF-NN
9: Apply O_{NN}, E, S to the adaptive VScontrol system
10: Prepare the control input u for the HDV system
11: Send u through the shared CANbus network

Simulations have been carried out for different attacks launched over the time. Effects of different attacker's dynamic functions and external disturbances are investigated in two cases, which are illustrated in Fig. 3. In Fig. 3(a) and (b), two examples of cyber attacks are depicted, which are sinusoidal and intermittent pulse attacks launched to damage the CPS system. The GRBFNN works as an intelligent estimator to estimate the attacker's dynamic function and disturbance. Estimations are depicted in Fig. 3(c) and (d). Moreover, the controlled speeds in the examples are shown in Fig. 3(e) and (f). It can be observed from Fig. 3(e) and (f) that the switching surfaces converge asymptotically to zero. Thus, the tracking aims are satisfied. The proposed control system maintains the stability of the HVD system. Simulations confirm that the proposed method is capable of controlling nonlinear CPS system in presence of attacks and external disturbances.

VI. Conclusion

In this article, we proposed a novel strategy to estimate and compensate attacks launched in the forward link of nonlinear CPSs using the intelligent VS control. The proposed strategy is a combination of nonlinear control and artificial NN. Nonlinear control theory was applied to guarantee stability and robustness of the CPS. Learning of the NN estimator was used for attack estimation, based on the adaptation law obtained by the Lyapunov stability proof, which, in turn, guarantees the stability of the closed-loop controlled CPS. Achievements of this article can be summarized as follows.

1) The proposed strategy is able to control the nonlinear CPSs while cyber attacks occur in the forward link.
2) The proposed control system can be applied to a variety of nonlinear CPSs, no matter how many dimensions the nonlinear CPS contains, because it is designed for n-order nonlinear systems.
3) The controller and estimator used in strategy are very popular.

4) The intelligent estimator works in an online manner and its learning rule is obtained through the Lyapunov stability proof.
5) The controller is robust against to cyber attacks in the forward link as well as external disturbances on the system. Simulations results confirm the efficiency of the proposed strategy when applied in the cruise control of an HVDS and the control.

References

[1] L. Monostori *et al.*, "Cyber-physical systems in manufacturing," *Corporate Insolvency Resolution Process Ann.*, vol. 65, no. 2, pp. 621–641, 2016.

[2] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security-a survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.

[3] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," *Comput. Sec.*, vol. 68, pp. 81–97, 2017.

[4] D. Ding, Q.-L. Han, Z. Wang, and X. Ge, "A survey on model-based distributed control and filtering for industrial cyber-physical systems," *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 2483–2499, May 2019.

[5] A. Bonci, M. Pirani, and S. Longhi, "Tiny cyber-physical systems for performance improvement in the factory of the future," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1598–1608, Mar. 2019.

[6] Y. Zhang, Z. Guo, J. Lv, and Y. Liu, "A framework for smart production-logistics systems based on CPS and industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4019–4032, Sep. 2018.

[7] A. Arabsorkhi, M. S. Haghighi, and R. Ghorbanloo, "A conceptual trust model for the internet of things interactions," in *Proc. 8th Int. Symp. Telecommun.*, 2016, pp. 89–93.

[8] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Syst.*, vol. 35, no. 1, pp. 110–127, Feb. 2015.

[9] A. Jolfaei and K. Kant, "Privacy and security of connected vehicles in intelligent transportation system," in *Proc. 49th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.–Supplemental Volume*, 2019, pp. 9–10.

[10] A. Jolfaei, K. Kant, and H. Shafei, "Secure data streaming to untrusted road side units in intelligent transportation system," in *Proc. 18th IEEE Int. Conf. Trust, Sec. Privacy Comput. Commun./13th IEEE Int. Conf. Big Data Sci. Eng.*, 2019, pp. 793–798.

[11] S. G. Ezabadi, A. Jolfaei, L. Kulik, and R. Kotagiri, "Differentially private streaming to untrusted edge servers in intelligent transportation system," in *Proc. 18th IEEE Int. Conf. Trust, Sec. Privacy Comput. Commun./13th IEEE Int. Con. Big Data Sci Eng.*, 2019, pp. 781–786.

[12] A. Mohammadali, M. S. Haghighi, M. H. Tadayon, and A. Mohammadi-Nodooshan, "A novel identity-based key establishment method for advanced metering infrastructure in smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2834–2842, Jul. 2018.

[13] A. Humayed and B. Luo, "Cyber-physical security for smart cars: Taxonomy of vulnerabilities, threats, and attacks," in *Proc. ACM/IEEE 6th Inter. Conf. Cyber-Physical Syst.*, 2015, pp. 252–253.

[14] H.-K. Kong, M. K. Hong, and T.-S. Kim, "Security risk assessment framework for smart car using the attack tree analysis," *J. Ambient Intell. Humanized Comput.*, vol. 9, no. 3, pp. 531–551, 2018.

[15] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Proc. Int. Workshop Hybrid Syst.: Comput. Control*, 2009, pp. 31–45.

[16] J.-Y. Keller and D. Sauter, "Monitoring of stealthy attack in networked control systems," in *Proc. Conf. Control Fault-Tolerant Syst.*, 2013, pp. 462–467.

[17] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. Commun., Control, Comput., Annu. Allerton Conf.*, 2009, pp. 911–918.

[18] A. O. de Sá, L. F. R. da Costa Carmo, and R. C. Machado, "Covert attacks in cyber-physical control systems," *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 1641–1651, Aug. 2017.

[19] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *Proc. 49th IEEE Conf. Decis. Control*, 2010, pp. 5967–5972.

[20] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical DC microgrids," *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2693–2703, Oct. 2017.

[21] F. Farivar and M. Aliyari, "Fault tolerant synchronization of chaotic heavy symmetric gyroscope systems versus external disturbances via lyapunov rule-based fuzzy control," *ISA Trans.*, vol. 51, no. 1, pp. 50–64, 2012.

[22] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1457, Jun. 2014.

[23] M. Corradini and A. Cristofaro, "A sliding-mode scheme for monitoring malicious attacks in cyber-physical systems," *IFAC Papers OnLine*, vol. 50, no. 1, pp. 2702–2707, 2017.

[24] M. L. Corradini and A. Cristofaro, "Robust detection and reconstruction of state and sensor attacks for cyber-physical systems using sliding modes," *IET Control Theory Appl.*, vol. 11, pp. 1756–1766, 2017.

[25] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proc. 49th IEEE Conf. Decis. Control*, 2010, pp. 5991–5998.

[26] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 667–674, Dec. 2011.

[27] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, "Stealthy deception attacks on water scada systems," in *Proc. ACM Int. Conf. Hybrid Syst., Comput. Control*, 2010, pp. 161–170.

[28] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water scada systems—Part I: Analysis and experimentation of stealthy deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 5, pp. 1963–1970, Sep. 2013.

[29] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen, "Cyber security of water scada systems—Part II: Attack detection using enhanced hydrodynamic models," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 5, pp. 1679–1693, Sep. 2013.

[30] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops*, 2008, pp. 495–500.

[31] W. Yan, L. K. Mestha, and M. Abbaszadeh, "Attack detection for securing cyber physical systems," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8471–8481, Oct. 2019.

[32] Y. Chen, S. Kar, and J. M. Moura, "Optimal attack strategies subject to detection constraints against cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 1157–1168, Sep. 2018.

[33] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[34] S. Nateghi, Y. Shtessel, J. Barbot, G. Zheng, and L. Yu, "Cyber-attack reconstruction via sliding mode differentiation and sparse recovery algorithm: Electrical power networks application," in *Proc. 15th Int. Workshop Variable Structure Syst.*, 2018, pp. 285–290.

[35] F. Farivar, M. S. Haghighi, S. Barchinezhad, and A. Jolfaei, "Detection and compensation of covert service-degrading intrusions in cyber physical systems through intelligent adaptive control," in *Proc. 20th IEEE Int. Conf. Ind. Technol.*, 2019, pp. 1143–1148.

[36] M. Sayad Haghighi, F. Farivar, A. Jolfaei, and M. H. Tadayon, "Intelligent robust control for cyber-physical systems of rotary gantry type under denial of service attack," *J. Supercomputing*, 2019, doi: 10.1007/s11227-019-03075-2.

[37] F. Farivar, M. A. Shoorehdeli, M. A. Nekoui, and M. Teshnehlab, "Synchronization of underactuated unknown heavy symmetric chaotic gyroscopes via optimal gaussian radial basis adaptive variable structure control," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 6, pp. 2374–2379, Nov. 2013.

[38] M. R. Kandroodi, F. Farivar, M. Z. Pedram, and M. A. Shoorehdeli, "Variable structure control and anti-control of flexible joint manipulator with experimental validation," in *Proc. IEEE Int. Conf. Mechatronics*, 2011, pp. 294–299.

[39] F. Farivar, M. A. Shoorehdeli, M. A. Nekoui, and M. Teshnehlab, "Chaos control and generalized projective synchronization of heavy symmetric chaotic gyroscope systems via gaussian radial basis adaptive variable structure control," *Chaos, Solitons Fractals*, vol. 45, no. 1, pp. 80–97, 2012.

[40] J.-J. E. Slotine and W. Li, *Applied Nonlinear Control*, vol. 199, no. 1. Englewood Cliffs, NJ, USA: Prentice-Hall, 1991.

[41] P. Kupsc, "Preceding vehicle dynamics modeling for fuel efficient control strategies," 2016.

Faezeh Farivar (M'16) received the Ph.D. degree in control systems from Science and Research Branch, Islamic Azad University, Tehran, Iran. She has been an Assistant Professor with the Department of Mechatronics and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran, since 2011. She was a Postdoc Research Fellow with the Department of Control Engineering, K. N. Toosi University of Technology from 2013 to 2016, and also with the Department of Machine Intelligence and Robotics, University of Tehran from 2011 to 2013. She has also been a Research Fellow with Research Institute of Robotics, Artificial Intelligence, and Information Science. She is the Subdirector of Advanced Networking and Security research Laboratory in robotics. Her research interests include nonlinear control systems, cyber-physical systems, and intelligent systems.

Mohammad Sayad Haghighi (SM'18) received the Ph.D. degree in telecommunication systems from K. N. Toosi University of Technology, Tehran, Iran. He is the Head of IT Department, School of Electrical and Computer Engineering, University of Tehran, Tehran, Iran. Prior to joining the University of Tehran, he was an Assistant Professor with Iran Telecom Research Center. Since 2009, he has been holding research positions with Australian Universities. He has done a postdoctoral study with Deakin University during 2012 and 2013. He has worked in senior positions for R&D companies, telecom companies, banks, and even governmental organizations up to the strategy definition level as a cyber security/IT consultant as well as an architect. He is the Director of Advanced Networking and Security Research Laboratory. He has had several positions in industry as well. His research interests include wireless ad hoc networks as well as cyber security.

Mr. Haghighi has served as a Program Committee Member of many conferences such as IEEE WNS, IEEE SICK, and IEEE LCN. He has won several national grants including one from Iran National Science Foundation.

Alireza Jolfaei (SM'19) received the Ph.D. degree in applied cryptography from Griffith University, Southport, QLD, Australia.

He is currently an Assistant Professor in Cyber Security with Macquarie University, Sydney, NSW, Australia. Prior to this appointment, he was an Assistant Professor with Federation University, Australia and Temple University in Philadelphia, PA, USA. His current research areas include cyber security, Internet of Things security, human-in-the-loop CPS security, cryptography, artificial intelligence, and machine learning for cyber security.

Dr. Jolfaei has received multiple awards for Academic Excellence, University Contribution, and Inclusion and Diversity Support. He is a Founding Member of Federation University IEEE Student Branch. He is an ACM Distinguished Speaker on the topic of Cyber-Physical Systems Security.

Mamoun Alazab (SM'17) received the Ph.D. degree in computer science from the School of Science, Information Technology and Engineering, Federation University of Australia, Mount Helen, VIC, Australia.

He is currently an Associate Professor with the College of Engineering, IT and Environment, Charles Darwin University, Casuarina, NT, Australia. He is also a Cyber Security Researcher and a Practitioner with industry and academic experience. He works closely with government and industry on many projects, including the Northern Territory (NT) Department of Information and Corporate Services, IBM, Trend Micro, the Australian Federal Police, etc. He is the Founder and the Chair of the IEEE NT Subsection Detection and Prevention. His research is multidisciplinary that focuses on cyber security and digital forensics of computer systems with a focus on cybercrime detection and prevention, including cyber terrorism and cyber warfare.