Resilient Nonlinear Control for Attacked Cyber-Physical Systems

Yan Pang, Hao Xia and Michael J. Grimble, *Fellow, IEEE*

***Abstract*—In this work, the problem of resilient nonlinear control for cyber-physical systems over attacked networks is studied. The motivation for this research comes from growing applications that demand the secure control of cyber-physical systems in industry 4.0. The nonlinear physical system considered can be attacked by changing the temporal characteristics of the network, causing fixed time or time-varying delays and changing the orders of received packets. The systems under attack can be destabilized if the controller is not designed to be robust with an adversarial attack. In order to cope with nonlinearity of the physical system, a Nonlinear Generalized Minimum Variance (NGMV) controller and a modified Kalman estimator are derived. A worst-case controller is presented for fixed-time delay. In the situations of time-varying delays and out-of-order transmissions, an opportunistic estimator and a resilient controller are designed through an on-line algorithm in the sense that it is calculated by using the information in the received packets immediately. The ability of use the received information immediately leads to the improvement of the controller's performance. Simulation results are provided to show the applicability and performance of control law developed.**

***Index Terms*—cyber-physical systems, delayed and out-of-order packets, nonlinear generalized minimum variance controller, worst-case estimation**

I. Introduction

A Cyber-Physical System (CPS) is a system which tightly integrates the computation, communication and physical control of plants [1]. The combination of physical system dynamics, software dynamics, and communications poses many challenges. The traditional control problem involves designing a robust and stable control law that provides best performance. The requirements change markedly when the total system including communications and networking are considered.

Security and resilience are critical issues of modern control systems that are subject to exogenous disturbances and open to random adversarial attacks or events. This realization leads to the emergence of new security challenges for control systems [2], [3], [4] that are different from traditional security problems. A Q-learning based optimal controller has been proposed which absorbs the cyber system states into the physical system model to derive a controller that can accommodate attacks using a zero sum game problem formulation [5]. A novel optimal control solution of the problem is presented below that accounts for the possible attacks and events, using a relatively simple control solution.

A typical security threat might involve the signal transmission, in a wireless networked control system, through delayed and out-of-order sensor communications [6]. Such delays and out-of-order transmission might be caused by network congestion, malicious relay nodes or poor connectivity in the network, intentionally delaying messages [7], [8]. This attack is called packet scheduling attacks in [9], when applied in the communication channel between the multiple sensors and the controller. In this work to prevent an adversary from changing the information of the packets, it was assumed that cryptographic algorithms could be used by all the network nodes to encrypt, decrypt and authenticate packets.

In classic control design the effects of delayed and missing measurements of data, has been considered from many aspects [10], [11]. There has been a number of papers on the effects of time delays, and data loss, on control systems after the introduction of NCS [12], [13], [14], [15], [16]. However, these approaches are not effective for CPSs with packet scheduling attacks for two reasons:

1) A fixed delay cannot be adaptable when there is actually no time delay in the real communication;
2) These methods may lose a lot of data when the sensors are sending out-of-order data.

Other work investigates the state estimation problem under out-of-order measurements [17], [18], [19] but the control of a physical system is not considered. Most of the effort for protecting CPSs has been on the reliability [20], but there is a growing concern for security under the malicious cyber-attacks [21], [22], [23], [24], [9].

It has been shown in [21] that the dynamic performance of frequency control in a power system is adversely affected by the communication delays. A stabilizing controller for smart

This research is supported by the National Natural Science Foundation of China (No.61004041,61273098) and the Fundamental Research Funds for the Central Universities (No.DUT16QY23). We are also grateful for cooperation with the University of Strathclyde in Glasgow, Scotland

Y. Pang is with the State Key Laboratory of Structural Analysis for Industrial Equipment, Dalian University of Technology, Dalian 116023, P.R. China, ypang@dlut.edu.cn

H.Xia (corresponding author) is with the School of Control Science and Engineering, Dalian University of Technology, P.R.China hao.x.xia@dlut.edu.cn

M.J.Grimble is with the Industrial Systems and Control Ltd., The Culzean Building, 36 Renfield Street, Glasgow G2 1LU, Scotland, United Kingdom m.grimble@isc-ltd.com

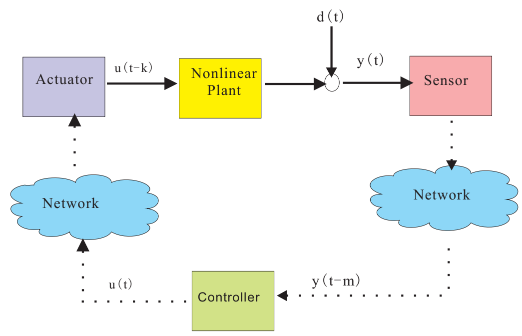


Fig. 1. A closed-loop single controller of cyber-physical systems with attacks on the network. A delay m affects sensor measurement and a delay k affects the control input

grid systems under severe fault or malfunction of protection devices was described in [22]. An adaptive framework for the control design of CPS in the presence of simultaneous adversarial sensor and actuator attacks was developed in [23]. It has been shown in [24] that process resilience to cyber-physical attacks can be improved through process-aware security analysis. A robust output feedback Linear-Quadratic-Gaussian (LQG) controller which is resilient to the packet scheduling attacks in networked control systems was presented in [9]. The LQG framework has been applied broadly for the security control of CPSs or networks, for example [25], [26], [27], [28], [29]. The assumption was that the control system is linear. However even approximately linear systems are very rare in the real physical world [30]. Resilient “nonlinear” control methodologies are therefore proposed in the following.

In order to deal with out-of-order communication and time-varying delays, an over-designed controller can be designed where all the packets are stored in a buffer and the controller will use the correct order after a fixed time delay. Obviously, this fixed time delay approach cannot provide a best performance of the controller. However, a controller can be designed using a worst-case control framework, as in [9] which assumed a linear system description.

The contribution of this paper may now be summarized. To achieve a better performance for the CPS under network packet scheduling attacks, an opportunistic design is applied to the nonlinear physical systems by appropriate choice of cost-function and system description. The approach uses a control algorithm that can accommodate non-linear systems and is relatively simple. Assuming a pre-defined operator equation has a stable inverse, the nonlinear system can be stabilized and optimized. The system can be represented by a state-dependent state-space model, a linear parameter varying model, transfer-operators, neural networks or even nonlinear function look-up tables. An opportunistic estimator and a resilient controller are designed using an on-line algorithm. The estimation and control performance of the observer-based controller is improved by implementing the online computing algorithm which is aware of possible attacks because of the system definition.

II. Problem Statement

A. Types of packet scheduling attacks

A networked CPS with a closed-loop single controller is illustrated in Fig1. The packet scheduling attacks try to change the temporal characteristics of the network. Therefore, sensor measurements data is transmitted through a network which has a delay of $m > 0$ in each of packets [31]. The control input data is delayed by $k > 0$ during the network transmission to the actuator. The delay is caused by the attacker's actions including network congestions, poor network connectivity or a malicious relay delaying data delivery. There are three attacker's scenarios with different effects that are discussed in this paper. They are: a fixed delay to the network, some loss of the packets and out-of-order packets.

Remark 2.1: The focus here is on resilient control under attack, not the behavior of the attacker. Therefore, the behavior of the attacker is not modeled. The attention is only on the effect e.g. a fixed delay, loss of the packets, or out-of-order packets. It is also assumed the attacker's behavior has to be kept stealthy and relative "subtle". In other work, for example [32], the model of the attacker is given. Based on this model, the attacker can even identify the optimal time to launch an attack and drive the system to an unsafe state. □

The output side scenarios are shown in Fig.2. The input side should have the same scenarios, however for simplicity assume the input side only has the fixed delay situation. Therefore, the focus of this paper is on the attacker's effect on the sensor measurements. In what follows, the three types of packet scheduling attacks for nonlinear systems are considered.

B. Problem Formulation

Consider the CPS shown in Fig.1, where the communication link connecting the sensor and the controller can be attacked. In order to restrict the capabilities of the attacker, the following assumption will be made:

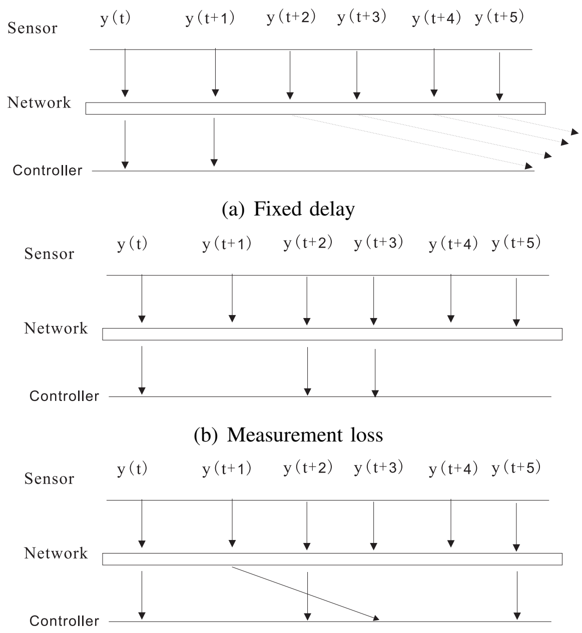
Assumption 2.1: It is assumed that the attacker is able to generate time-varying delays. However, a packet can only be delayed no more than τ^* time units.

This assumption is not restrictive because the attacker has to be kept stealthy then he will not delay a packet by a very long time.

The physical plant is described by a nonlinear discrete-time system

$$\begin{aligned} x(t+1) &= f(x(t), u(t-k), d(t)) \\ y(t+1) &= g(\alpha_t x(t), v(t)) \end{aligned} \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state, $u(t) \in \mathbb{R}^m$ is the control with $m \leq n$. The disturbances $d(t)$ and measurement noise $v(t)$ are independent zero-mean random vectors. It was assumed that input side only have the fixed delay, then $u(t-k)$ is used



(a) Fixed delay

(b) Measurement loss

(c) Variable dealy

Fig. 2. An adversarial attack affecting packet delivery scenarios from sensor to controller transmissions.

to define the fixed k time unit delay in the input side. While the sensor measurement may have out-of-order communication and time-varying delays defined by the parameter α_t:

$$\alpha_t = \begin{cases} 0 & if\ there\ is\ no\ packet\ recieved\ at\ time\ t \\ 1 & if\ the\ packet\ is\ transmitted\ correctly \\ & \quad at\ time\ t \\ z^{-m_t} & if\ the\ packet\ is\ delayed\ by\ m_t\ time\ unit \end{cases} \tag{2}$$

where $m_t \in \mathbb{N}$ is a varying time delay caused by the network attacker.

The objective is to design an optimal controller which is resilient to the packet scheduling attack. The behavior of the attacker, i.e. preventing the transmission of the packet, or changing the order of the packets, is aimed at preventing the controller observing the exact state. The control strategy must therefore be robust to the worst case disturbance that is compatible with the received sequence of observations. The general framework in [33] is followed to design such a feedback NGMV controller where the cost function J is defined in a minimum variance sense. The optimal NGMV control problem can be presented as the minimization of signal $\{\phi_c\}$:

$$\phi_c = P_c e(t) + (\mathcal{F}_c u)(t) \tag{3}$$

where $e(t)$ defines the error signal of the system (1). The signal $\{\phi_c\}$ includes an error signal dynamic cost weighting operator: $P_c(z^{-1})$, described by a linear state-space subsystem and a nonlinear dynamic control costing operator $(\mathcal{F}_c u)(t)$. Choosing the dynamic weightings is critical to the design of the system; normally P_c is low-pass while $\mathcal{F}_c$ is high-pass. We define the cost function J in terms of the signal $\{\phi_c\}$ as

$$J = E\{\phi_c^T(t)\phi_c(t)\} = E\{trace\{\phi_c^T(t)\phi_c(t)\}\} \tag{4}$$

where $E\{\cdot\}$ denotes the expectation operator.

The resilient control design can be split into two parts: firstly an observer which estimates the worst possible state, using the sequence of available inputs and output signals, has to be designed; secondly a nonlinear controller which uses the estimated state has to be derived. From above procedure, the worst case state estimator can be described as follows. Whenever an out-of-order packet is available to the estimator, it starts by reordering the sequences of previous N messages, calculates the worst case disturbance which is compatible with the available information, finds the corresponding worst case state estimate. The nonlinear controller can be computed immediately the estimated state is available. The details about how to construct the worst case observer and the nonlinear controller under the specified network attack are discussed in the next two sections.

III. Non-linear controller design

In order to design the output feedback controller for the proposed CPSs, we consider the physical system has a nonlinear plant in a more general form than the system (1). In addition to the nonlinear physical plant model, defined in (1), it is assumed that the system also includes a disturbance model, a reference model and a linear model. The disturbance and reference signals are assumed to have linear forms. This assumption is not very restrictive, as the models of the disturbance and references are only approximations in most applications.

A. A general nonlinear model of physical system

A general form for the discrete-time system including the nonlinear physical plant and the linear disturbance and reference models, is described in Fig. 3. The plant model includes a general non-linear model $\mathcal{W}_{1k}$, which is assumed to be finite gain stable. The output of the nonlinear block is assumed to feed a linear subsystem, denoted by W_{0k}, which can be open-loop unstable. If such a block is not present, then it can be set equal to the identity. The disturbance and reference models are assumed to be represented by linear subsystems.The measurement disturbance defined as $\{v(t)\}$ can be the attack action in the network. Without loss of generality, it is assumed that the zero-mean, white noise signals $\{\xi_0\}$ and $\{\xi_d\}$ have identity covariance matrices. It is not necessary to specify the distribution of the noise sources, because of the special structure of the system which leads to a prediction equation, which is dependent on the "linear" disturbance and reference models. The signals in Fig. 3 are shown as follows:

- Error signal: $e(t) = r(t) - y(t)$
- Plant output: $y(t) = d(t) + (\mathcal{W}u)(t)$
- Reference: $r(t) = W_r \omega(t)$
- Output disturbance: $d(t) = W_d \xi_d(t)$
- Observations signal:$o(t) = y(t) + v(t)$
- Disturbed error signal: $e_0(t) = r(t) - o(t)$

The system has separate reference and disturbance models associated with each set of delayed outputs. These subsystems

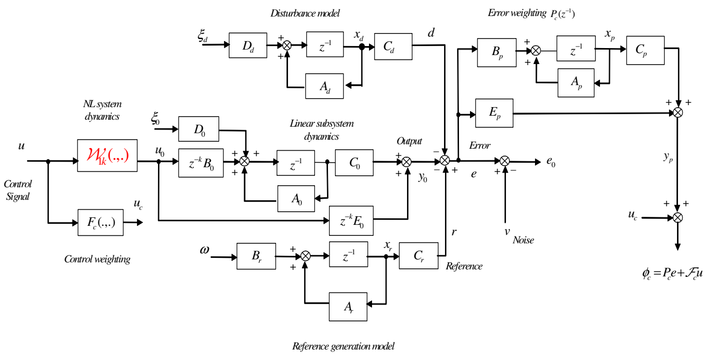


Fig. 3. Nonlinear, linear, reference, error weighting and disturbance submodels

are therefore assumed to be in block diagonal form. State-space matrix system models and nonlinear operator models may be listed as follows:

- Reference model:

$$x_r(t+1) = A_r x_r(t) + B_r \omega(t) \quad (5)$$
$$r(t) = C_r x_r(t) \quad (6)$$

where $x_r(t) \in \mathbb{R}^{n_r}$, $\omega(t)$ is the reference signal .

- Disturbance model:

$$x_d(t+1) = A_d x_d(t) + D_d \xi_d(t) \quad (7)$$
$$d(t) = C_d x_d(t) \quad (8)$$

where $x_d(t) \in \mathbb{R}^{n_d}$.

- Linear plant:

$$x_0(t+1) = A_0 x_0(t) + z^{-k} B_0 u_0(t) + D_0 \xi_0(t) \quad (9)$$
$$y_0(t) = C_0 x_0(t) + z^{-k} E_0 u_0(t) \quad (10)$$
$$W_0(z^{-1}) = C_0(zI - A_0)^{-1} z^{-k} B_0 + z^{-k} E_0 \quad (11)$$

where $x_0(t) \in \mathbb{R}^{n_0}$.

- Error weighting:

$$x_p(t+1) = A_p x_p(t) + B_p e(t) \quad (12)$$
$$y_p(t) = C_p x_p(t) + E_p e(t) \quad (13)$$

where $x_p(t) \in \mathbb{R}^{n_p}$ and

$$e(t) = C_r x_r(t) - C_d x_d(t) - C_0 x_0(t) - z^{-k} E_0 u_0(t) \quad (14)$$

- Nonlinear model: the total plant model can be described as

$$\mathcal{W}(t) = z^{-k} \mathcal{W}_k(t) = z^{-k} W_{0k} \mathcal{W}_{1k}(t) \quad (15)$$

z^{-k} denotes the input delay operator caused by the attacks of the network between controller and the actuator shown in Fig 1 in the control paths and note that this operator commutes with others which may be a problem for time varying operators or LPV.

- Combined state-space model: By combining the linear systems in this section (except (15)), the augmented state equations for the total system are obtained as

$$x(t+1) = Ax(t) + Bu_0(t-k) + D\xi(t) \quad (16)$$
$$y(t) = Cx(t) + Eu_0(t-k) \quad (17)$$
$$y_p(t) = C_\phi x(t) + E_\phi u_0(t-k) \quad (18)$$
$$e_0(t) = C_e x(t) - z^{-k} E_0 u_0(t) - v(t) \quad (19)$$

where $x(t) = [\ x_0^T \quad x_d^T \quad x_r^T \quad x_p^T\ ]^T$ and $x(t) \in \mathbb{R}^{n_0+n_d+n_r+n_p}$. Let $n = n_0 + n_d + n_r + n_p$ then $x(t) \in \mathbb{R}^n$. A, B, C_ϕ, E_ϕ and C_e are defined accordingly, see [34] for details.

Let $\Psi = (zI - A)^{-1}$ define the resolvent operator, and the transfer operator form of the linear subsystem $W_{0k} = E_0 + C\Psi B = E_0 - C_e \Psi B$.

Note that in (15) the linear system W_{0k} is represented by a general state-space model described in (9)-(11), but the nonlinear system is not necessarily assumed to be available in a known equation form. An operator $\mathcal{W}_{1k}$ is therefore used to describe the "black-box" nonlinear system. According to [33], $\mathcal{W}_{1k}$ can be a very general nonlinear operator, which could involve state-dependent state-space models, transfer operators, neural networks or even nonlinear function look-up tables. Also, it should be noted that the the error signal and noise e_0 is a function of $x(t)$ and $v(t)$. These both include uncertain signals/parameters that can be treated as being due to the action of the attacker.

B. NGMV control

Consider the equation (3) again, the control signal costing is defined to have the following form:

$$(\mathcal{F}_c u)(t) = z^{-k} (\mathcal{F}_{ck} u)(t) \quad (20)$$

It is assumed that the control weighting operator $\mathcal{F}_{ck}$ is full rank and invertible. In the set of channels with delay k steps, the control signal affects the outputs $\phi_c(t)$ at least k steps later. The expression for $\phi_c(t)$ after a k -step delay can be expressed using (3) as

$$\begin{aligned}\phi_c(t+k) &= P_c e(t+k) + (\mathcal{F}_{ck} u)(t) \\ &= C_\phi x(t+k) + E_\phi u_0(t) + (\mathcal{F}_{ck} u)(t)\end{aligned} \quad (21)$$

where $u_0 = (\mathcal{W}_{1k} u)(t)$, so that:

$$\phi_c(t+k) = C_\phi x(t+k) + E_\phi (\mathcal{W}_{1k} u)(t) + (\mathcal{F}_{ck} u)(t) \quad (22)$$

Assumption 3.1: It will be assumed that the nonlinear subsystem $\mathcal{W}_{1k}$ is stable, any unstable models in the plant are only appeared in the linear subsystem W_{0k}.

Theorem 3.1: Under the assumption 3.1, the optimal control input signal u (shown in Fig. 4), when the cost function J in equation (4) is minimized in a variance sense, can be obtained as:

$$u(t) = -(\mathcal{F}_{ck} + (C_\phi T_0(k, z^{-1}) B + E_\phi) \mathcal{W}_{1k})^{-1} C_\phi A^k \hat{x}(t|t) \quad (23)$$

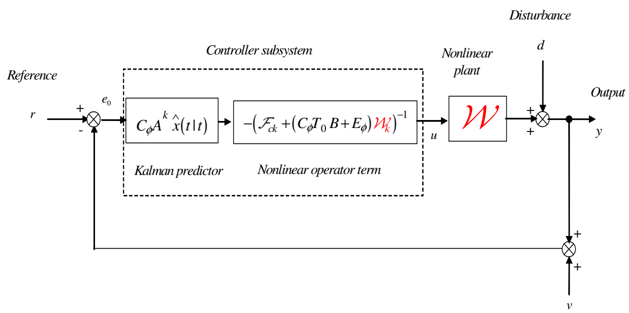


Fig. 4. NGMV controller structure

Proof: The variance $J = \{\phi_c^T(t)\phi_c(t)\}$ in equation (4) can be presented in terms of the prediction $\hat{\phi}_c(t+k|t)$ with the prediction error $\tilde{\phi}_c(t+k|t)$. From the orthogonality principle:

$$J = E\{\hat{\phi_c}^T(t+k|t)\hat{\phi}_c(t+k|t)\} + E\{\tilde{\phi_c}^T(t+k|t)\tilde{\phi}_c(t+k|t)\} \tag{24}$$

The prediction error $\tilde{\phi}_c(t+k|t)$ has no relation with the control signals, so the minimization of the cost J is to set the prediction $\hat{\phi}_c(t+k|t) = 0$. Considering equation (22), the optimal control signal is obtained by solving the following equation:

$$\begin{aligned}\hat{\phi}_c(t+k|t) &= C_\phi \hat{x}(t+k|t) + E_\phi(\mathcal{W}_{1k}u)(t) + (\mathcal{F}_{ck}u)(t) \\ &= 0\end{aligned} \tag{25}$$

where $\hat{x}(t+k|t)$ is k-steps ahead of the state estimates of the combined system in (16). It has the following forms:

$$\hat{x}(t+k|t) = A^k \hat{x}(t|t) + T_0(k, z^{-1})Bu_0(t) \tag{26}$$

where

$$T_0(k, z^{-1}) = (I - A^k z^{-k})\Psi \tag{27}$$

Hence, the equation (25) is written as follows:

$$C_\phi(A^k \hat{x}(t|t) + T_0(k, z^{-1})Bu_0(t)) + (E_\phi \mathcal{W}_{1k} + \mathcal{F}_{ck})u(t) = 0 \tag{28}$$

In Fig.3, it is clear that the input in (28) $u_0 = (\mathcal{W}_{1k}u)(t)$ then the optimal $u(t)$ can be expressed as in (23) $\square$

Another expression of $T_0(k, z^{-1})$ is as follows:

$$T_0(k, z^{-1}) = z^{-1}(I + z^{-1}A + z^{-2}A^2 + ... + z^{-(k-1)}A^{k-1}) \tag{29}$$

In order to simplify notation, T_0 is used to define $T_0(k, z^{-1})$.

C. Modified Kalman filter state estimation equations

In Theorem 3.1, the state estimation of $\hat{x}(t|t)$ can be obtained via a modified Kalman filter. Before introducing the Kalman filtering equations for the system, a parameter can be introduced, according to whether the packet is received or not. The parameter α_t is simplified to the packet loss parameter $\gamma_t \in \{0, 1\}$, where

$$\gamma_t = \begin{cases} 1 & if \quad there\ is\ a\ packet\ received\ at\ time\ t \\ 0 & otherwise \end{cases}$$

Although the optimal control problem includes the non-linear input subsystem, the state estimator is linear. The Kalman filter acts on the plant observations, which include the effects of both noise and control signal inputs. The effect of control action can be removed easily. This enables the predicted value of state due to stochastic inputs to be obtained and then the effect of the known control inputs can be recovered by adding an appropriate term. To demonstrate these results consider the standard Kalman system and estimator structure, but modified to take account of the special explicit delay structure of the system.

Plant model:

$$x(t+1) = Ax(t) + z^{-k}Bu_0(t) + D\xi(t) \tag{30}$$

$$o(t) = Cx(t) + z^{-k}E_0u_0(t) \tag{31}$$

Error signal:

$$\begin{aligned}e_0(t) &= r(t) - y(t) - v(t) = r(t) - Cx(t) - z^{-k}E_0u_0(t) - v(t) \\ &= C_e x(t) - z^{-k}E_0u_0(t) - v(t)\end{aligned} \tag{32}$$

Predictor-corrector form estimator:

$$\hat{x}(t+1|t) = A\hat{x}(t|t) + z^{-k}Bu_0(t) \quad (Predictor) \tag{33}$$

$$\hat{x}(t+1|t+1) = x(t+1|t) + \gamma_t K_f(e_0(t+1) - \hat{e}_0(t+1|t)) \quad (Corrector) \tag{34}$$

Note that $\hat{e}_0 = C_e x(t+1|t) - z^{-k}E_0u_0(t+1)$

$$\begin{aligned}\hat{x}(t+1|t+1) &= \hat{x}(t+1|t) + \gamma_t K_f(e_0(t+1) \\ &- C_e\hat{x}(t+1|t) + z^{-k}E_0u_0(t+1))\end{aligned} \tag{35}$$

$$\begin{aligned}\hat{x}(t+1|t+1) &= (A - \gamma_t K_f C_e A)\hat{x}(t|t) + z^{-k}Bu_0(t) \\ &+ \gamma_t K_f(e_0(t+1) - C_e z^{-k}Bu_0(t) + z^{-k}E_0u_0(t+1))\end{aligned} \tag{36}$$

Let $z^{-1}\hat{x}(t+1|t+1) = \hat{x}(t|t)$ then $\hat{x}(t|t)$ is as follows:

$$\begin{aligned}\hat{x}(t|t) &= (I - z^{-1}(A - \gamma_t K_f C_e A))^{-1}(z^{-k-1}Bu_0(t) \\ &+ \gamma_t K_f(e_0(t) + z^{-k}E_0u_0(t) - C_e z^{-k-1}Bu_0(t))\end{aligned} \tag{37}$$

The k steps ahead prediction due to the stochastic inputs can be written as: $A^k x(t|t)$ and the total predicted output, assuming u_0 is known k steps ahead, is given as:

$$\begin{aligned}\hat{x}(t+k|t) &= A^k\hat{x}(t|t) + A^{k-1}Bu_0(t-k) + A^{k-2}Bu_0(t-k+1) \\ &+ ... + ABu_0(t-2) + Bu_0(t-1)\end{aligned} \tag{38}$$

It can be seen that equations (38) and (26) are the same with the function T_0 defined in (27).

D. Stability

In order to analyze the stability of the proposed controller, a different expression of (23) is given firstly.

$$u(t) = -\mathcal{F}_{ck}^{-1}(C_\phi A^k \hat{x}(t|t) + (C_\phi T_0 B + E_\phi) \times (\mathcal{W}_{1k}u)(t)) \tag{39}$$

According to $\gamma_t = 0$ or 1, $\hat{x}(t|t)$ has different expressions.

(1)$\gamma_t = 0$

In this case, if the contribution of the control signal is not considered, then the Kalman filter output, when the effect of control action is removed, has the form:

$$\hat{x}_{dr}(t|t) = \hat{x}(t|t) - (zI - A)^{-1}Bu_0(t-k) \tag{40}$$

Recalling $\Psi = (zI - A)^{-1}$, we have the predicted output:

$$\hat{x}(t+k|t) = A^k \hat{x}_{dr}(t|t) + \Psi B u_0(t) \tag{41}$$

and the prediction of ϕ_c

$$\begin{aligned}\hat{\phi}_c(t+k|t) &= C_\phi(A^k\hat{x}_{dr}(t|t) + \Psi B u_0(t)) + ((E_\phi \mathcal{W}_{1k} + \\ &\quad \mathcal{F}_{ck})u)(t) \\ &= C_\phi A^k \hat{x}_{dr}(t|t) + (E_\phi + C_\phi \Psi B)\mathcal{W}_{1k}u(t) + \mathcal{F}_{ck}u(t)\end{aligned} \tag{42}$$

Note that $P_c W_{0k} = E_\phi + C_\phi \Psi B$

$$\hat{\phi}_c(t+k|t) = C_\phi A^k \hat{x}_{dr}(t|t) + (P_c\mathcal{W}_k + \mathcal{F}_{ck})u(t) \tag{43}$$

Let $\hat{\phi}_c(t+k|t) = 0$, the optimal control has the form:

$$u(t) = -(P_c\mathcal{W}_k + \mathcal{F}_{ck})^{-1}C_\phi A^k \hat{x}_{dr}(t|t) \tag{44}$$

If the observations are null for a period the response of $\hat{x}_{dr}(t|t)$ will be due to initial condition response from the point at which the measurements are lost.

(2)$\gamma_t = 1$

$$\begin{aligned}\hat{x}(t|t) =& (I - z^{-1}(A - K_f C_e A))^{-1}(z^{-k-1}Bu_0(t) \\ &+ K_f(e_0(t) + z^{-k}E_0u_0(t) - C_e z^{-k-1}Bu_0(t)))\end{aligned} \tag{45}$$

According to (39), the control signal can be written as:

$$\begin{aligned}u(t) = &-\mathcal{F}_{ck}^{-1}(C_\phi A^k(I - z^{-1}(A - K_f C_e A))^{-1} \\ &(z^{-k-1}Bu_0(t) + K_f(e_0(t) + z^{-k}E_0u_0(t) - \\ &C_e z^{-k-1}Bu_0(t))) + (C_\phi T_0 B + E_\phi) \times (\mathcal{W}_{1k}u)(t))\end{aligned} \tag{46}$$

Recall $T_0 = (I - A^k z^{-k})\Psi$,$W_{0k} = E_0 - C_e\Psi B$, $C_\phi \Psi B + E_\phi = -P_c W_{0k}$ and $x(t) = z^{-k}\Psi B u_0 + \Psi D\xi(t)$, the above equation can be written as:

$$\begin{aligned}u(t) = &-\mathcal{F}_{ck}^{-1}(C_\phi A^k(I - z^{-1}(A - K_f C_e A))^{-1}K_f \\ &(r(t) - C\Psi D\xi(t) - v(t))) - P_c W_{0k}u_0(t)\end{aligned} \tag{47}$$

In order to analyze the stability, it is assumed that the exogenous inputs, except the reference signal $r(t)$, are null. Then the optimal control signal can be written as:

$$\begin{aligned}u(t) = &(P_c\mathcal{W}_k - \mathcal{F}_{ck})^{-1}(C_\phi A^k(I - z^{-1}(A \\ &- K_f C_e A))^{-1}K_f r(t)\end{aligned} \tag{48}$$

According to [34], the series connections of two finite gain M_2 stable systems is also M_2 stable. It can be seen that in either case (44) or (48) the condition of system stability is that the operator $(P_c\mathcal{W}_k - \mathcal{F}_{ck})^{-1}$ is finite gain M_2 stable. This can be achieved by choosing the weightings that ensure the existence of the stable non-linear operator inverse. It is therefore an assumption that the weightings are chosen to satisfy this requirement which in linear system terms is to assume the operator $(P_c\mathcal{W}_k - \mathcal{F}_{ck})$ is minimum-phase.

IV. Resilient Controller design

Since the packet scheduling attacks have different types shown in Fig 2, the worst-case control strategies are needed. For whatever types of attacks, the worst-case estimation process may take the following steps:

- store all the past received data
- use all of the available data to compute the worst-case uncertain parameters
- estimate the worst-case system state
- upgrade the control input
- apply the control action to the system and repeat from step one

In the three types of packet scheduling attacks, the first type where the system is attacked under fixed delay is relative simple. Therefore, the optimal control under fixed delay is introduced firstly.

A. Optimal control under fixed delay

Consider a piece of sensor's data with fixed delay $m_t = \tau$ (τ is a constant), whose timescale is defined by $t \in [0, N]$, where N is a natural number. The time delay is fixed at $m_t = \tau$ and $N - \tau \geq 1$, that means from time 0 to N only up to $N - \tau$ is transmitted to the controller, while in the next $t \in [N-\tau+1, N]$ time steps there is no information available to the controller. For example, Fig. 2 (a) shows a transmission under the fixed time delay, where $N = 5, \tau = 4$, there are two situations:

- (a) from initial time to $N - \tau = 1$ the controller has received information normally and the observation is available. The control design for this period is the same as the no time delay format.
- (b) from time $N-\tau+1 = 2$ to $N = 5$ the controller has no information received and no observation is available. The control design for this period should follow the estimation under the worst-case.

From above analysis, we have the following theorem that can solve the optimal control problem under fixed delay.

Assumption 4.1: Given a piece of sensor's data with fixed time delay $m_t = \tau$, whose timescale is defined by $t \in [0, N]$. In order to guarantee that there are some packets are transmitted correctly, it is assumed that the fixed delay time has to satisfy $N - \tau \geq 1$. Therefore the upper bound of time delay in assumption 2.1 has satisfy $\tau^* \leq N - 1$.

Theorem 4.1: Consider a nonlinear plant defined in sectionIII-A and a fixed delay $m_t = \tau$ under the assumption 4.1. If the operator $(P_c\mathcal{W}_k - \mathcal{F}_{ck})^{-1}$ is finite-gain stable, the optimal controller can be designed where:

1) if $t \in [0, N - \tau]$, then $\gamma_t = 1$ and the estimator is closed-loop and takes the form (36);
2) if $t \in [N - \tau + 1, N]$, then $\gamma_t = 0$ and the estimator is open-loop and takes the form (33);
3) feedback controller (23) is for all $t \in [0, N]$.

Proof: Under the assumption 4.1, the proof is as follows.

1) from assumption 4.1, during the period $t \in [0, N-\tau]$ all the data are transmitted correctly, therefore the optimal control problem is a normal state feedback NGMV control problem.
2) otherwise during $t \in [N-\tau+1, N]$, there are no transmissions arrived, the optimal control problem is an open-loop NGMV control problem
3) under the assumption $(P_c\mathcal{W}_k - \mathcal{F}_{ck})^{-1}$ is finite-gain stable, controller (23) can be either closed-loop ($\gamma_t = 1$) or open-loop ($\gamma_t = 0$).

□

Remark 4.1: Theorem 4.1 shows that if there is a stable solution for NGMV control, there is always an estimator to take either the closed-loop form or the worst-case open-loop form and the controller can be updated based on these estimation results. For the attack under time varying delay or out-of-order situations it is still possible to use Theorem 4.1 by picking up an artificial fixed delay τ before the time-varying delay or out-of-order appears. This involves using the open-loop estimation during $t \in [N-\tau+1, N]$ for whatever information is received, or not, during $t \in [N-\tau+1, N]$. □

However, for the time-varying delay or out-of-order cases the forced open-loop estimation is conservative and the resulting controller is over-designed. Hence, an opportunistic estimator and a resilient controller for time-varying delay and out-of-order packets is derived in the next section.

B. Optimal control under time-varying delay and out-of-order packets

The packet scheduling attacks actually affect the temporal order of the sensor data at each time instant. The delay time m_t can be time-varying. This has motivated the design of a dynamic estimator that take into account the history of the packet losses or mixed orders. Under the influence of these attacks, the dynamic updated estimator and the optimal controller should optimize the worst-case performance.

The following sets needed for the algorithm to be defined:

- The original number of the current received packet
$$R(t) = \begin{cases} \{n_y^j\} & if\ there\ is\ a\ packet\ received\ at\ time\ t \\ \phi & otherwise \end{cases}$$
where n_y^j is a random number in $\{0, 1..., N\}$ and $\{0, 1, ..., N\}$ is the sequnces of the sensor sending out data. If mitiple packets are recieved at the same time insterval, $R(t)$ is the set of all the number n_y^j . The set of orignal numbers received by the controller until time $m > 0$ is defined as $\mathcal{R}_0^m = \{R(t)|t \in [0, m]\}$;
- The current measurement received by the controller
$$\bar{y}(t) = \begin{cases} \{y(n_y^j)\} & if\ R(t) = n_y^j \\ \phi & if\ R(t) = \phi \end{cases}$$
The set of all measurements recieved by the controller by time m is $\bar{\mathcal{Y}}_0^m = \{\bar{y}(t)|t \in [0, m]\}$;
- The control sequence $\{u(0), ..., u(m-1)\}$ and the state estimation sequence $\{\hat{x}(0), ..., \hat{x}(m)\}$ are defined as $\bar{\mathcal{U}}_0^{m-1}$ and $\bar{\mathcal{X}}_0^m$ respectively.

The opportunistic resilient controller can be implemented by following algorithm. In order to reduce the computational effort, the following conditions are assumed.

Assumption 4.2: It is assumed that there is a time period $N - \tau \geq 1 (\tau > 0)$ that for $t \in [0, N-\tau]$ all the information is transmitted correctly eg. $\alpha_t = 1$. Therefore the upper bound of time delay in assumption 2.1 has satisfy $\tau^* \leq N - 1$.

Then our focus in following algorithm will be given on the time period $[N-\tau+1, N]$ where the time-varying delay and out-of-order transmissions may appear. The number of packets received at each time interval is defined as n_y^j. Buffers $\mathcal{R}_0^m$,$\bar{\mathcal{Y}}_0^m$ and $\bar{\mathcal{U}}_0^{m-1}$ of appropriate sizes are defined for storing the information. In addition buffers $\bar{\mathcal{X}}_0^m$ is created to store the state-estimate $\hat{x}(t)$. The values of all buffers are stored in ascending order of their transmission time. When a measurement is unavailable to the controller at a particular time t, then its buffer value is empty. The Algorithm 4.1 below describes the steps for an implementation of the proposed resilient controller.

Algorithm 4.1:

Initialize $\mathcal{R}_0^{N-\tau+1}, \bar{\mathcal{Y}}_0^{N-\tau+1}, \bar{\mathcal{U}}_0^{N-\tau}, \bar{\mathcal{X}}_0^{N-\tau}$
 based on the real system paramerters
for $t = (N-\tau) : N$
 $R(t+1) \leftarrow$ according to packets received at $[t, t+1]$
 if $R(t+1) = \phi$
  $\gamma_{t+1} := 0$
  $\hat{x}(t+1|t+1) \leftarrow$(33)
  $\bar{y}(t+1) := \phi$
 else
  update $\bar{\mathcal{Y}}_0^{t+1}$ according to $\bar{y}(R(t+1))$
  $i = min_j R(t+1)$
  $\hat{x}(i-1|i-1) := \bar{\mathcal{X}}(i-1)$
  for $l = i-1 : t$
   $u(l) := \bar{\mathcal{U}}(l)$
   $\bar{y}(l) := \bar{\mathcal{Y}}(l)$
   if $\bar{y}(l) = \phi$
    $\gamma_l = 0$
    $\hat{x}(l+1|l+1) \leftarrow$(33)
   else
    $\gamma_l = 1$
    $\hat{x}(l+1|l+1) \leftarrow$(36)
   end if
   update $\bar{\mathcal{X}}_0^{l+1}$
  end for
 end if
  $u(t+1) \leftarrow$(23)
  update $\bar{\mathcal{U}}_0^{t+1}$
end for

Theorem 4.2: If the assumptions in assumption 4.2 and theorem 4.1 hold, the opportunistic estimator and the resilient controller under the varying-time delay or out-of-order transmissions then can be designed by:

1) if $t \in [0, N-\tau]$, then $\alpha_t = 1$ and the estimator is closed-loop and takes the form (36);
2) if $t \in [N-\tau+1, N]$, then follow the algorithm 4.1;
3) feedback controller (23) is for all $t \in [0, N]$.

Proof: For $t \in [0, N-\tau]$ all the measurements received and the controller design is the same as in theorem 4.1. For $t \in [N-\tau+1, N]$, according to packet reception, the computation or re-computation of the optimal controller is updated online using the spirit of [35]. The controller is the same as the theorem 4.1, hence it is sufficient to prove that the estimator performed in algorithm 4.1 generates the opportunistic state estimation under the packet scheduling attack.

Let $y_i, i = 0, ..., N$ define the $i-th$ output signal the sensor sending out and Δ_i is the delay time function of receiving signal y_i

$$\Delta_i : \begin{cases} = 0 & if\ there\ is\ no\ time\ delay \\ \leq \tau & if\ there\ is\ a\ time\ delay \\ = \infty & if\ the\ singal\ is\ missing \end{cases}$$

Define $\eta_t(y_i, \Delta_i)$ as

$$\eta_t(y_i, \Delta_i) = \begin{cases} y_i & if\ t-i = \Delta_i \\ 0 & otherwise \end{cases} \quad (49)$$

For the CPS under the packet scheduling attack, at each time t the observer records the received and their correct order. The the output signal $y(t)$ can be expressed as:

$$y(t) = \{\eta_t(y_i, \Delta_i)\}_{i=0,...N} \quad (50)$$

The algorithm lines 10-23 can be seen as on-line dynamic multiple runs of the observer in theorem 4.1 over each $\eta_t(y_i, \Delta_i)$. Note there may be multiple packets received at the same time interval, then the observer's update should start from the earliest sent out signal $y(i_{min})$. Thus, the algorithm 4.1 generates the opportunistic state estimate, and the resilient controller to the packet scheduling attack. □

V. Rotational Link Control Problem

The proposed controller is applied to the control of a rotational link shown in Fig.5. This is a common problem in mechanisms. The example is rather artificial, since a real CPS can be a much larger system. However, there are few restrictions on the nonlinear plant, and the results of this work can be extended to other larger CPSs.

This system can be viewed as a simplified robotic manipulator with flexible joints. The controller communicates with the system through a wireless network, therefore a cyber-physical system is results. The motor torque should be controlled so that the motor rotates through a specified angle, whilst stabilizing vibration of the robot or mechanism arm. The rotational link is a highly nonlinear system where a nonlinear controller is required. A DC motor is used to rotate the link in the vertical plane. The equilibrium condition is defined to be the angle $\theta = \pi$, where the arm is straight down. The objective is to control the motor such that the link is stabilized at some desired angles. That is, the torque $T(t)$ is applied at

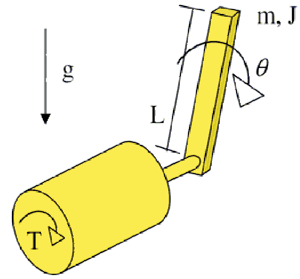


Fig. 5. Rotational Link

the rotational link so that the angular position θ follows a desired trajectory θ_{ref} . This system has one control input $u(t) = T(t)$, which is the torque that accelerates the link, that is generated by the motor [36]. The continuous-time dynamics of the system follow as:

$$\frac{d}{dt} = \begin{bmatrix} \theta(t) \\ \dot{\theta}(t) \end{bmatrix} = \begin{bmatrix} \dot{\theta}(t) \\ mgL\sin(\theta(t)/J - c\dot{\theta}|\theta| + u(t)) \end{bmatrix} \quad (51)$$

Let angular position θ be taken as the first system state. The continuous-time state-variables can then be defined as $x_1(t) = \theta$ and $x_2(t) = \dot{\theta}$, where $x(t) = [x_1(t), x_2(t)]^T = [\theta(t), \dot{\theta}(t)]^T$ The angle output $y(t) = [1 \ \ 0]x(t)$ and the approximate discrete nonliear model can be obtained as:

$$x(t+1) = \begin{bmatrix} 1 & T_s \\ \frac{T_s mgL\sin x_1}{Jx_1} & 1 - T_s c|x_2| \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ T_s \end{bmatrix} \quad (52)$$

A high sample rate is assumed with sample period $T_s = 0.01$. The numerical values for the parameters are $m = 1, g = 9.81, L = 0.5, J = 0.25, c = 5$. The cost weightings are:

$$P_c = \frac{0.165 - 0.155z^{-1} + 0.04z^{-2}}{1 - 1.5z^{-1} + 0.5z^{-2}} \quad (53)$$

The control weighting is defined as:

$$F_{ck} = -1(1 + 0.1z^{-1}) \quad (54)$$

In the simulations, simulation time $T = 14$ seconds. The reference angular position is:

$$r(t) = \begin{cases} \pi & 0 \leq t \leq 7 \\ \frac{3}{4}\pi & 7 \leq t \leq 14 \end{cases}$$

The proposed controller is simulated with and without packet scheduling attacks. The results are compared in Fig 6. The black line is the system response when there is no attack. If there are fixed delays with $\tau = 0.5s$ that happens at $t = 1s$ and $t = 7s$, an output of this over-designed estimator/controller (in section IV-A)is shown by the green line. If we consider the delay time and transmission orders are random, the output of the proposed controller, defined by Algorithm 4.1 and Theorem 4.2 is shown in the blue line. The performance has been improved after using the proposed controller.

VI. Conclusions

A resilient controller for a cyber-physical system subject to attacks has been presented for a rather general nonlinear

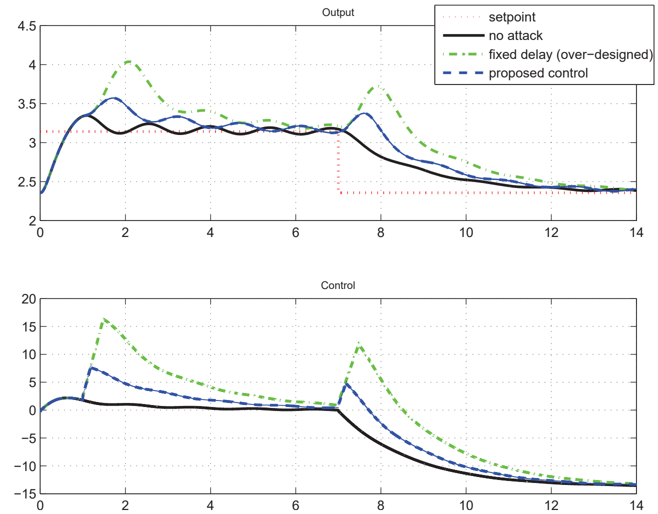


Fig. 6. The output and control input for three different cases evaluated

physical plant. To treat the nonlinearity of the system, a nonlinear generalized minimum variance controller and a modified Kalman estimator have been derived. Three types of packet scheduling attacks were considered namely fixed-time delay, time-varying delay and out of-order transmissions and these were treated differently. A worst-case controller for a fixed-time delay has been designed. In the time-varying delay and out-of-order transmissions situations, an opportunistic estimator and a resilient controller have been designed. This involved a dynamic by a dynamic algorithm 4.1, in the sense that it is designed by using the information in the packets just received immediately. The ability to immediately use the information received brings an improvement in the control performance.

The proposed controller has been evaluated in a nonlinear rotational link system application, where a malicious node introduced time-varying delay and out-of-order packet delivery. Simulation results demonstrate the performance of the estimator and the robustness of the resilient controller.

In the future, the results are easy to extend to the case where there are also attacks on the input side (between the controller and the actuators). Clearly, as the attacks are occurring randomly, the stochastic uncertainty that models the unknown, and the unanticipated events, have to be taken into consideration. These effects are included in the system description and the optimal solution then accommodates these special characteristics of cyber-physical systems. For the future the Nonlinear Predictive Generalized Minimum Variance (NPGMV) controller without black box term could be easy to implement and solve the same problem. One can use the prediction capability to handle attacks on the way. For example, future disturbance knowledge can be used just like future reference knowledge. Thus, if a future attack can be modeled by a disturbance then the future knowledge is very useful.

REFERENCES

[1] K.-D. Kim and P. R. Kumar, "Cyber-physical systems: A perspective at the centennial," *Proceedings of the IEEE*, vol. 100, no. special Centennial-Issue, pp. 1287 – 1308, 2012.

[2] S. Amin, A. A. Cardenas, and S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *In R. Majumdar and P. Tabuada, editors, Hybrid Systems: Computation and Control* ,, Springer Berlin Heidelberg, 2009.

[3] K. Vamvoudakis, J. Hespanha, B. Sinopoli, and Y. Mo, "Detection in adversarial environments," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3209–3223, 2014.

[4] J. Hendrickx, K. Johansson, R. Jungers, H. Sandberg, and K. C. Sou, "Efficient computations of a security index for false data attacks in power networks," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3194–3208, 2014.

[5] H. Niu and S. Jagannathan, "Optimal defense and control for cyber-physical systems," in *2015 IEEE Symposium Series on Computational Intelligence*, Cape Town, South Africa, 2015.

[6] L. Shi, P. Cheng, and J. Chen, "Sensor data scheduling for optimal state estimation with commu- nication energy constraint," *Automatica*, vol. 47, no. 8, pp. 1693–1698., 2011.

[7] W. Kang, K. Kapitanova, and S. H. Son, "RDDS: A real-time data distribution service for cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 8, no. 2, pp. 393–405, 2012.

[8] L. X. Zhang, Z. P. Ning, and Z. D. Wang, "Distributed filtering for fuzzy time-delay systems with packet dropouts and redundant channels," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 46, no. 4, pp. 559–572, 2016.

[9] Y. Shoukry, J. Araújo, P. Tabuada, M. Srivastava, , and K. H. Johansson, "Minimax control for cyber-physical systems under network packet scheduling attacks," in *In Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems*, 2013.

[10] K. Åstrom and B. Wittenmark, Eds., *Computer controlled systems*. Prentice Hall Englewood Cliffs, NJ, 1990.

[11] T. Glad and L. Ljung, Eds., *Control Theory: Multivariable and Nonlinear Methods.* Taylor & Francis, 2000.

[12] W. Zhang, M. S. Branicky, and S. M. Phillips, "Stability of networked control systems," *IEEE Control Systems Magazine*, vol. 21, no. 1, pp. 84–99., 2001.

[13] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 138–162, 2007.

[14] T. Yang, "Networked control system: a brief survey. control theory and application," *IEE Proceedings*, vol. 153, no. 4, pp. 403–412, 2006.

[15] J. Araújo, "Design, implementation and validation of resource-aware and resilient wireless networked control systems," Ph.D. dissertation, KTH Royal Institute of Technology, 2014.

[16] P. Lee, A. Clark, L. Bushnell, and R. Poovendran, "A passivity framework for modeling and mitigating wormhole attacks on networked control systems," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3224–3237, 2014.

[17] J. Wu, Q. Jia, K. H. Johansson, and L. Shi, "Event-based sensor data scheduling: Trade-off between communication rate and estimation quality," *IEEE Transactions on Automatic Control*, vol. 58, no. 4, pp. 1041–1046, 2013.

[18] Y. Bar-Shalom, "Update with out-of-sequence measurements in tracking: exact solution," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 38, no. 3, pp. 769–777, 2002.

[19] K. Zhang, X. Li, and Y. Zhu, "Optimal update with out-of-sequence measurements," *IEEE Transactions on Signal Processing*, vol. 53, no. 6, pp. 1992–2004, 2005.

[20] D. Zhang, H. Song, and L. Yu, "Robust fuzzy-model-based filtering for nonlinear cyber-physical systems with multiple stochastic incomplete measurements," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 47, no. 8, pp. 1826–1838, 2017.

[21] S. Liu, X. Wang, and P. X. Liu, "Impact of communication delays on secondary frequency control in an islanded microgrid," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 4, pp. 2021–2031, 2015.

[22] A. Farraj, E. Hammad, and D. Kundur, "A cyber-enabled stabilizing control scheme for resilient smart grid systems," *IEEE Transactions on Smart Grid*, vol. 4, no. 7, pp. 1856–1865, 2016.

[23] X. Jin, W. M. Haddad, and T. Yucelen, "An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 11, pp. 6058–6064, 2017.

[24] M. Krotofil and A. A. Cárdenas, "Resilience of process control systems to cyber-physical attacks," in *In Proceedings of the 18th Nordic Conference, NordSec 2013, Lecture Notes in Computer Science, Springer,*, pp. 166–182.

[25] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. Sastry, "Foundations of control and estimation over lossy networks," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 163 – 187, 2007.

[26] E. Garone, B. Sinopoli, A. Goldsmith, and A. Casavola, "LQG control for mimo systems over multiple erasure channels with perfect acknowledgment," *IEEE Transactions on Automatic Control*, vol. 57, no. 2, pp. 450–456, 2012.

[27] M. Trivellato and N. Benvenuto, "State control in networked control systems under packet drops and limited transmission bandwidth," *IEEE Transactions on Communications*, vol. 58, no. 2, pp. 611– 622, 2012.

[28] Q. Zhu and T. Başar, "Robust and resilient control design for cyber-physical systems with an application to power systems," in *Proceedings of the IEEE Conference on Decision and Control,*, Orlando, FL, 2011.

[29] H. Zhang, P. Cheng, L. Shi, , and J. Chen, "Optimal denial-of-service attack scheduling against linear quadratic gaussian control." in *Proceedings of American Control Conference*, Portland, OR, 2014.

[30] Y. Yuan, Z. Wang, and L. Guo, "Event-triggered strategy design for discrete-time nonlinear quadratic games with disturbance compensations: The noncooperative case," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, In Press.

[31] Z. Gao, T. Breikin, and H. Wang, "Reliable observer-based control against sensor failures for systems with time delays in both state and input," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 38, no. 5, pp. 1018–1029, 2008.

[32] M. Krotofil, A. A. Cárdenas, J. Larsenc, and D. Gollmann, "Vulnerabilities of cyber-physical systems to stale data-determining the optimal time to launch attacks," *International Journal of Critical Infrastructure Protection*, vol. 7, no. 4, pp. 213–232, 2014.

[33] M. J. Grimble, "Non-linear generalized minimum variance feedback, feedforward and tracking control," *Automatica*, vol. 6, no. 41, pp. 957–969, 2005.

[34] ——, "GMV control of non-linear continuous-time systems including common delays and state-space models," *International Journal of Control*, vol. 1, no. 80, pp. 150–165, 2007.

[35] J. Moon and T. Başar, "Control over lossy networks: A dynamic game approach," in *Proceedings of the American Control Conference*, 2014.

[36] A. Shawky, A. Ordys, and M. Grimble, "End-point control of a flexible-link manipulator using h-ifinity nonlinear control via a state-dependent riccati equation," in *Proceedings of the IEEE Conference on Control Applications*, Glasgow, UK, 2002.

Yan Pang received the PhD degree from the University of Strathclyde, at Glasgow, UK in 2004. She is currently an Associate Professor with the School of Aeronautics and Astronautics, Dalian University of Technology. Prior to that, she was a Research Associate with the Sheffield University, UK and a Research Fellow with the University of Strathclyde, UK. Her current research interests include system and control theory, control of hybrid and nonlinear systems, and resilient control of CPSs.

Hao Xia received the Ph.D. degrees in Electrical Engineering from the University of Birmingham, U.K. in 2000. He is currently a Professor with the School of Control Science and Engineering, Dalian University of Technology. Prior to that, he was a principal automation engineer with GlaxoSmithKline. His current research interests include control system performance assessment and advance process control.

Michael J. Grimble BSc, BA, MSc, PhD, DSc, CEng, Fellow IEEE, Fellow IET, Fellow IMA, Fellow Inst. M.C, Fellow of Royal Society of Edinburgh. Mike Grimble established the Industrial Control Centre at the University of Strathclyde over 30 years ago following his experience on the Industrial Automation Group at Imperial College. He also established a company, Industrial Systems and Control Limited which is a leading advanced control consultancy and is heavily involved in industrial projects and training courses mostly in the United States and UK. He acts as the Technical Director and Deputy Chairman of ISC Ltd., and also established the Applied Control Technology Consortium which included companies from around the world. He is the Managing Editor of three journals published by John Wiley on advanced control and is also the joint Editor of a Springer Monograph Series on Advances in Industrial Control, and a Springer Textbook Series on Control and Signal Processing.