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 of 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.

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 China (No.61004041,61273098 ) and the Fundamental Research Funds for the Central Universities (No.DUT16QY23). We are also grateful for cooperation China (No.61004041,61273098 ).

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

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
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.

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 Fig.1. 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 $\tau^*$ 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

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

(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.
and a nonlinear dynamic control costing operator \((J)\). We define the cost function \(P\) operator:

\[
J = E\{\phi_c^T(t)\phi_c(t)\} = E\{\text{trace}\{\phi_c^T(t)\phi_c(t)\}\}
\]

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 \(W_{1,k}\), which is assumed to be finite gain stable. The output of the nonlinear block is assumed to feed a linear subsystem, denoted by \(W_{0,k}\), 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: \(y(t) = d(t) + (Wu)(t)\)
- Reference: \(r(t) = W\omega(t)\)
- Output disturbance: \(d(t) = W\xi_d(t)\)
- 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
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:
  \[
  x_r(t + 1) = A_r x_r(t) + B_r \omega(t) \]
  \[
  r(t) = C_r x_r(t)
  \]
  where \( x_r(t) \in \mathbb{R}^{n_r} \), \( \omega(t) \) is the reference signal.

- Disturbance model:
  \[
  x_d(t + 1) = A_d x_d(t) + D_d \xi_d(t)
  \]
  \[
  d(t) = C_d x_d(t)
  \]
  where \( x_d(t) \in \mathbb{R}^{n_d} \).

- Linear plant:
  \[
  x_0(t + 1) = A_0 x_0(t) + z^{-k} B_0 u_0(t) + D_0 \xi_0(t)
  \]
  \[
  y_0(t) = C_0 x_0(t) + z^{-k} E_0 u_0(t) \]
  \[
  W_0(z^{-1}) = C_0 (zI - A_0)^{-1} z^{-k} B_0 + z^{-k} E_0
  \]
  where \( x_0(t) \in \mathbb{R}^{n_0} \).

- Error weighting:
  \[
  x_p(t + 1) = A_p x_p(t) + B_p c(t)
  \]
  \[
  y_p(t) = C_p x_p(t) + E_p c(t)
  \]
  where \( x_p(t) \in \mathbb{R}^{n_p} \) and
  \[
  c(t) = C_r x_r(t) - C_d x_d(t) - C_0 x_0(t) - z^{-k} E_0 u_0(t)
  \]

- Nonlinear model: the total plant model can be described as
  \[
  W(t) = z^{-k} W_k(t) = z^{-k} W_{0k} W_{1k}(t)
  \]
  \( z^{-k} \) 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
  \[
  x(t + 1) = A x(t) + B u_0(t - k) + D \xi(t)
  \]
  \[
  y(t) = C x(t) + E u_0(t - k)
  \]
  \[
  y_p(t) = C_p x(t) + E_p u_0(t - k)
  \]
  \[
  c_0(t) = C_c x(t) - z^{-k} E_0 u_0(t) - v(t)
  \]
  where \( x(t) = [x_0^T \ x_d^T \ x_r^T \ x_p^T]^T \) 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 \( x(t) \in \mathbb{R}^n \). \( A, B, C_p, E_p \) and \( C_c \) 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 \( W_{0k} = E_0 + C \Psi B = E_0 - C \Psi B \).
  
  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 \( W_{1k} \) is therefore used to describe the "black-box" nonlinear system. According to [33], \( W_{1k} \) 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:
  \[
  (F_c u)(t) = z^{-k} (F_{ck} u)(t)
  \]
  It is assumed that the control weighting operator \( F_{ck} \) 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
  \[
  \phi_c(t + k) = P_c x(t + k) + (F_{ck} u)(t)
  \]
  \[
  = C_0 x(t + k) + E_0 u_0(t) + (F_{ck} u)(t)
  \]
  where \( u_0 = (W_{1k} u)(t) \), so that:
  \[
  \phi_c(t + k) = C_0 x(t + k) + E_0 (W_{1k} u)(t) + (F_{ck} u)(t)
  \]
  \( Assumption 3.1: \) It will be assumed that the nonlinear subsystem \( W_{1k} \) 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:
  \[
  u(t) = -(F_c + (C_0 T_0(k, z^{-1}) B + E_0) W_{1k})^{-1} C_0 A^k \hat{x}(t)|t
  \]
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 account for the special explicit delay structure of the system.

**Plant model:**

\[
x(t + 1) = Ax(t) + z^{-k}Bu_0(t) + D\xi(t)
\]

\[
o(t) = Cx(t) + z^{-k}E_0u_0(t)
\]

**Error signal:**

\[
e_0(t) = r(t) - y(t) - v(t) = r(t) - Cx(t) - z^{-k}E_0u_0(t) - v(t)
\]

**Predictor-corrector form estimator:**

\[
h\hat{x}(t\mid t + 1) = \hat{x}(t) + z^{-k}Bu_0(t) \quad \text{(Predictor)}
\]

\[
h\hat{x}(t + 1) = h\hat{x}(t\mid t) + \gamma_0K_1(e_0(t + 1) - \hat{e}_0(t)) \quad \text{(Corrector)}
\]

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

\[
h\hat{x}(t\mid t) = \left(1 - A^k z^{-k}\right)\Psi
\]

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

\[
T_0(k, z^{-1}) = \left(1 + z^{-1} \right)^{-1} \sum_{k=0}^{\infty} A^k z^{-k-1}
\]

\[
r(t) = u(t) + \gamma(t) + \xi(t)
\]

\[
\gamma(t) = \left\{ \begin{array}{ll} 1 & \text{if there is a packet received at time } t \\ 0 & \text{otherwise} \end{array} \right.
\]

Although the optimal control problem includes the nonlinear input subsystem, the state estimator is linear. The

**Proof:** The variance \(J = \{\phi_T(t)\phi_c(t)\}\) in equation (4) can be presented in terms of the prediction \(\hat{c}(t + k|t)\) with the prediction error \(\phi_c(t + k|t)\). From the orthogonality principle:

\[
J = E\{\hat{c}^T(t + k|t)\hat{c}(t + k|t)\} + E\{\hat{c}^T(t + k|t)\phi_c(t + k|t)\}
\]

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

\[
\hat{c}(t + k|t) = C_0\hat{x}(t + k|t) + E_0(W_{1k}u)(t) + (\mathcal{F}_{ck}u)(t)
\]

\[
= 0
\]

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:

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

where

\[
T_0(k, z^{-1}) = (I - A^k z^{-k})\Psi
\]

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

\[
C_0(A^k\hat{x}(t|t) + T_0(k, z^{-1})Bu_0(t)) + (E_0W_{1k} + \mathcal{F}_{ck})u(t) = 0
\]

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

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

\[
T_0(k, z^{-1}) = z^{-1}(I + z^{-1} A + z^{-2} A^2 + \ldots + z^{-(k-1)} A^{k-1})
\]

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

\[
C_{\text{mod}} = \left\{ \begin{array}{ll} 1 & \text{if there is a packet received at time } t \\ 0 & \text{otherwise} \end{array} \right.
\]

\[
\gamma_t = \left\{ \begin{array}{ll} 1 & \text{if there is a packet received at time } t \\ 0 & \text{otherwise} \end{array} \right.
\]
Recalling control action is removed, has the form:
\[ \hat{x}(t|t) = \hat{x}(t|t) - (I - A)^{-1}Bu(t - k) \]  
(40)
Recalling \( \Psi = (I - A)^{-1} \), we have the predicted output:
\[ \hat{x}(t + k|t) = A^k\hat{x}(t|t) + \Psi Bu(t) \]  
(41)
and the prediction of \( \phi_c \)
\[ \hat{\phi}_c(t + k|t) = C_\phi(A^k\hat{x}(t|t) + \Psi Bu(t)) + ((E_\phi W_{1k} + F_{ck})u(t) ) \]
\[ = C_\phi A^k\hat{x}(t|t) + (E_\phi + C_\phi \Psi B)W_{1k}u(t) + F_{ck}u(t) \]  
(42)
Note that \( P_cW_{0k} = E_\phi + C_\phi \Psi B \)
\[ \hat{\phi}_c(t + k|t) = C_\phi A^k\hat{x}(t|t) + (P_cW_{0k} + F_{ck})u(t) \]  
(43)
Let \( \hat{\phi}_c(t + k|t) = 0 \), the optimal control has the form:
\[ u(t) = -(P_cW_{0k} + F_{ck})^{-1}C_\phi A^k\hat{x}(t|t) \]  
(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.

\[ (2) \gamma_t = 1 \]
\[ \hat{x}(t|t) = (I - z^{-1}(A - K_f C_\phi A))^{-1}(z^{-k-1}Bu(t) \]
\[ + K_f(e_0(t) + z^{-k}E_0u_0(t) - C_\phi z^{-k-1}Bu_0(t)) \]  
(45)
According to (39), the control signal can be written as:
\[ u(t) = -F_{ck}^{-1}(C_\phi A^k(I - z^{-1}(A - K_f C_\phi A))^{-1} \]
\[ (z^{-k-1}Bu_0(t) + K_f(e_0(t) + z^{-k}E_0u_0(t) - C_\phi z^{-k-1}Bu_0(t)) + (C_\phi T_0B + E_\phi)\times(W_{1k}u(t)) \]  
(46)
Recall \( T_0 = (I - A^kz^{-k})\Psi W_{0k} = E_0 - C_\phi \Psi B, C_\phi \Psi B + E_\phi = -P_cW_{0k} \) and \( x(t) = z^{-k}\Psi Bu_0 + \Psi D \xi(t) \), the above equation can be written as:
\[ u(t) = -F_{ck}^{-1}(C_\phi A^k(I - z^{-1}(A - K_f C_\phi A))^{-1}K_f \]
\[ (r(t) - C_\phi D \xi(t) - v(t)) - P_cW_{0k}u_0(t) \]  
(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:
\[ u(t) = (P_cW_{0k} - F_{ck})^{-1}(C_\phi A^k(I - z^{-1}(A - K_f C_\phi A))^{-1}K_f r(t) \]  
(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 \( (P_cW_{0k} - F_{ck})^{-1} \) 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 \( (P_cW_{0k} - F_{ck}) \) is minimum-phase.

### IV. Resilient Controller Design

Since the packet scheduling controller 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 \( m_t = \tau \) (\( \tau \) 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 \( \tau \), 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 section III-A and a fixed delay \( m_t = \tau \) under the assumption 4.1. If the operator \( (P_cW_{0k} - F_{ck})^{-1} \) 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 \( t \in [0, N] \).
Theorem 4.1: If there is a stable delay and out-of-order transmissions may appear. The number of packets received at each time interval is defined as \( n_y^t \). Buffers \( R_0^m, \bar{Y}_0^m \) and \( \bar{U}_0^m \) of appropriate sizes are defined for storing the information. In addition buffers \( X_0^m \) 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, 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:**

1. Initialize \( R_0^m, \bar{Y}_0^m, \bar{U}_0^m, X_0^m \) based on the real system parameters
2. for \( t = (N - \tau) : N \)
3. \( R(t+1) \leftarrow \) according to packets received at \([t, t+1]\]
4. if \( R(t+1) = \phi \)
5. \( \gamma_{t+1} := 0 \)
6. \( \hat{x}(t+1|t+1) \leftarrow (33) \)
7. \( \tilde{y}(t+1) := \phi \)
8. else
9. update \( \bar{Y}_0^t \) according to \( \bar{y}(R(t+1)) \)
10. \( i = \min_i R(t+1) \)
11. \( \hat{x}(i-1|i-1) := \bar{X}(i-1) \)
12. for \( l = i - 1 : t \)
13. \( u(l) := \bar{U}(l) \)
14. \( \bar{y}(l) := \bar{Y}(l) \)
15. if \( \bar{y}(l) = \phi \)
16. \( \gamma_l = 0 \)
17. \( \hat{x}(l+1|l+1) \leftarrow (33) \)
18. else
19. \( \gamma_l = 1 \)
20. \( \hat{x}(l+1|l+1) \leftarrow (36) \)
21. end if
22. update \( \bar{X}_0^{t+1} \)
23. end for
24. end if
25. \( u(t+1) \leftarrow (23) \)
26. update \( \bar{U}_0^{t+1} \)
27. 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 trans-
missions 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 \( \Delta_i \) is the delay time function of receiving signal \( y_i \).

\[
\Delta_i : \begin{cases} 
0 & \text{if there is no time delay} \\
\leq \tau & \text{if there is a time delay} \\
\infty & \text{if the signal is missing}
\end{cases}
\]

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

\[
\eta_t(y_i, \Delta_i) = \begin{cases} 
y_i & \text{if } t - 1 = \Delta_i \\
0 & \text{otherwise}
\end{cases}
\]  

(49)

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

\[
y(t) = \{ \eta_t(y_i, \Delta_i) \}_{i=0,...,N}
\]  

(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 \( y(t_{\text{min}}) \). Thus, the algorithm 4.1 generates the opportunistic state estimate, and the resilient controller to the packet scheduling attack.

\[ \square \]

**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 the rotational link so that the angular position \( \theta \) follows a desired trajectory \( \theta_{\text{ref}} \). 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:

\[
d \frac{d}{dt} = \begin{bmatrix} \theta(t) \\ \dot{\theta}(t) \end{bmatrix} = \begin{bmatrix} 0 \\ mgL \sin(\theta(t)) - c \dot{\theta} + u(t) \end{bmatrix}
\]  

(51)

Let angular position \( \theta \) 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 \( y(t) = [1, 0]^T \) and the approximate discrete nonlinear model can be obtained as:

\[
x(t+1) = \begin{bmatrix} \frac{1}{T_s m g L \sin x_1} & \frac{T_s}{1 - T_s c |x_2|} \\ 1 - T_s c |x_2| \end{bmatrix} x(t) + \begin{bmatrix} 0 \\ T_s \end{bmatrix}
\]  

(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:

\[
P_c = \frac{0.165 - 0.155 z^{-1} + 0.04 z^{-2}}{1 - 1.5z^{-1} + 0.5z^{-2}}
\]  

(53)

The control weighting is defined as:

\[
F_{ck} = -1(1 + 0.1 z^{-1})
\]  

(54)

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

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

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...
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.

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

**References**


