2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Feedback Path Delay Attacks and Detection

Torbjörn Wigren and André Teixeira

Abstract— **The paper discusses delay injection attacks on regulator loops and suggests joint recursive prediction error identification of delay and dynamics for supervision and attack detection. The control system is assumed to be operated either in open- or closed-loop mode. It is shown why delay insertion in the feedback path before the user switches to closed-loop operation is advantageous to disguise the attack. The detection performance is evaluated numerically for a linearized automotive cruise control feedback loop.**

I. INTRODUCTION

Delay is a major enemy of feedback that limits performance and may cause instability [1], [2], [3]. The present paper observes that delay injection can also be a powerful tool for cyber attacks on feedback regulator systems. Mitigation means are therefore proposed, using joint recursive prediction error identification of loop delay and dynamics for supervision and early attack detection.

Cyber attacks on feedback controllers have proved to be efficient in the past, see the discussion on STUXNET in [4]. Such attacks on control systems have been extensively discussed in the literature and include, for example, deception [5], denial-of-service [6], and replay [7]. The present paper is however focused on the intentional injection of delay into the feedback loop. Protection against such attacks requires development and deployment of prevention, supervision, detection, and mitigation schemes, c.f. [8]. The classical literature on dynamic systems with delay provide general tools of analysis, see for example [1] and [3], as well as general methods to estimate delays [9]. The mitigation of delay injection attacks have been addressed by robust controller design [10], in particular for smart grids [11], [12]. However, the detection of delay attacks has only been subject to limited discussion, for example in [13], [14], [15]. Remaining gaps of knowledge include, for example, the conditions for detectability of delay attacks in open- and closed-loop, as well as the need for *online* robust detection algorithms tailored to such attacks

The paper [16] discusses delay attacks on networked servo control systems and corresponding detection schemes. Important additional questions posed and answered by the present paper include how delay attacks may be performed on closed-loop *regulators*, and how a successful detection of such attacks can be designed. As compared to the servo control problem, the detection challenges in closed-loop may be more significant, since the regulation objective tends to suppress signal variations useful for detection.

This work is supported by the Swedish Foundation for Strategic Research.

T. Wigren and A. Teixeira are with the Department of Information Technology, Uppsala University, SE-75105 Uppsala, Sweden. {torbjorn.wigren,andre.teixeira}@it.uu.se.

In the paper, this research problem is formulated for a general setup with linear time-invariant single-input-single-output (SISO) plant dynamics, subject to linear quadratic Gaussian regulation (LQG) with integral action, cf. [2], [17]. A specific property of the considered control loop is that the user selects between open-loop and closed-loop operation. The first question is then: how is the attack best applied and disguised? The questions for the defender treated in the paper are: how should a robust online detection of the delay attack be designed and what performance is obtained?

The paper first contributes with an analysis that imply opportunities to disguise the delay attack if the delay injection is performed in the feedback path of the regulator. Secondly, the paper contributes with delay attack supervision and detection by joint recursive prediction error identification of loop delay and open loop dynamics. The third contribution illustrates a disguised delay attack and the proposed delay attack detection method, when applied to a linearized automotive cruise control loop [18], [19]. Linear quadratic (LQ) control is used in this example.

It was shown in [9] that off-line output error identification algorithms perform the best when delay and dynamics are jointly identified. This is why the recursive prediction error method (RPEM) of [20] is applied for supervision and attack detection. However, identification of delay is a classical research subject. Potential alternatives to [20] may, for example, be based on time domain impulse response delay estimation [21], frequency domain methods [22], or higher order statistics [23].

The paper is organised with the description of the control loop in Section II. Delay injections attacks and their detection are discussed in Sections III and IV. Sections V and VI apply the methods of Sections III and IV to an automotive cruise control regulator. Conclusions follow in Section VII.

II. CONTROL SYSTEM

A. Block Diagram

The control system is depicted in the block diagram of Fig. 1. It consists of a standard linear state-space-based control loop. The formulation follows [2] and avoids stochastic ODEs, since delay attack and detection aspects are not affected by this choice. The focus is on the regulator problem.

The distinguishing feature of the control loop of Fig. 1 is the user-controlled switch between open-loop and closed-loop operation. Such a switch is, for example, found in adaptive cruise control (ACC) functionality [18], [19], [24].

The regulated system is assumed to be described by

$$\begin{aligned} \dot{\bar{\mathbf{x}}}(t) &= \bar{\mathbf{A}}\bar{\mathbf{x}}(t) + \bar{\mathbf{B}}\bar{u}(t) + \bar{\mathbf{w}}(t) \\ \bar{y}(t) &= \bar{\mathbf{C}}\bar{\mathbf{x}}(t) + \bar{e}(t). \end{aligned} \tag{1}$$

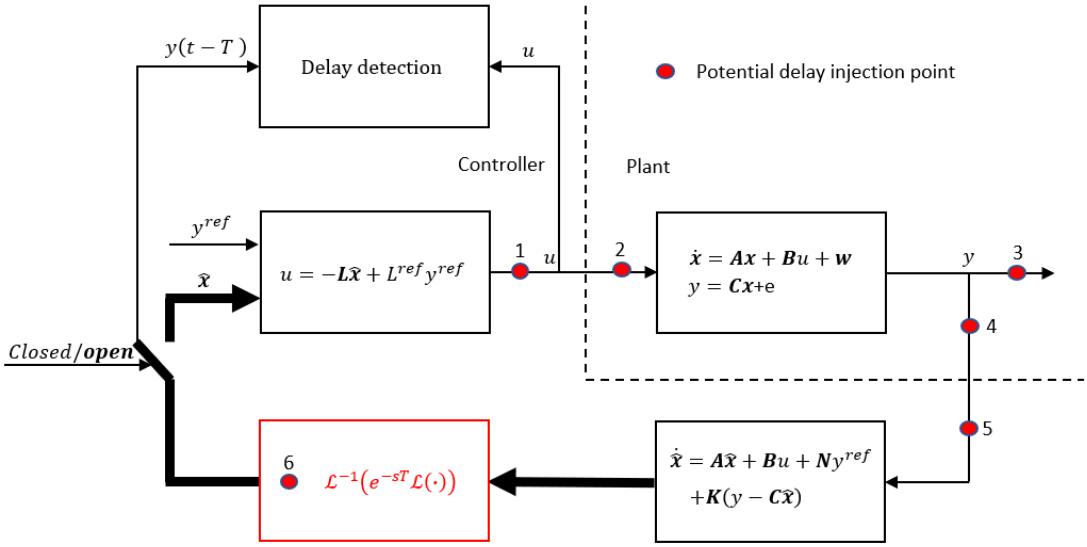

Fig. 1. The LQG regulator block diagram of the paper, with the preferred delay attack alternative 6 shown in red. T denotes the injected delay.

Here the overhead bar is used to distinguish w.r.t the state of the augmented model below that has an additional integrator state. As usual, $\bar{\mathbf{x}}(t) \in \mathbb{R}^n$ is the state vector, t is the time, $\bar{u}(t) \in \mathbb{R}^1$ is the control signal, $\bar{y}(t) \in \mathbb{R}^1$ is the output signal and $\hat{\bar{\mathbf{x}}}(t) \in \mathbb{R}^n$ is the estimated state vector, given measurements up to time t. Furthermore, $\bar{\mathbf{w}}(t) \in \mathbb{R}^n$ is the systems noise, and $\bar{e}(t) \in \mathbb{R}^1$ is the measurement noise. The matrices $\bar{\mathbf{A}}$ and $\bar{\mathbf{B}}$ are the system and input matrices, while $\bar{\mathbf{C}}$ is the measurement matrix.

B. Integrating Control

Since the regulator problem is addressed, handling of unmodelled disturbances with nonzero mean is a pre-requisite, which implies that integrating control is needed. This is achieved by augmentation of the state $\bar{\mathbf{x}}(t)$ with an integrator state using the differential equation,

$$\dot{x}_{n+1}(t) = -\delta x_{n+1} + \left(y^{ref}(t) - \bar{\mathbf{C}}\bar{\mathbf{x}}(t)\right). \tag{2}$$

Here $y^{ref}(t)$ is the reference signal.

Remark 1: The small $\delta > 0$ in (2) is needed to ensure detectability according to assumption A4 below. Note that this avoids a singular inverse caused by rank loss of $\mathbf{A}$ in (27). Since the components of $\mathbf{B}$ and $\tilde{\mathbf{z}}(t)$ equal 0 for the integrator state, it follows that $u(t)$ of (34) will become independent of δ, c.f. section VI.B. Integrating control is obtained when $\delta \to 0$. The use of $\bar{\mathbf{C}}\bar{\mathbf{x}}(t)$ instead of $y(t)$ is standard when applying state feedback from estimated states.

After the augmentation

$$\mathbf{x}(t) = \left(\bar{\mathbf{x}}^T(t) \quad x_{n+1}(t)\right)^T, \tag{3}$$

the system equations are transformed to the standard form

$$\begin{aligned} \dot{\mathbf{x}}(t) &= \mathbf{A}\mathbf{x}(t) + \mathbf{B}u(t) + \mathbf{N}y^{ref}(t) + \mathbf{w}(t) \\ y(t) &= \mathbf{C}\mathbf{x}(t) + e(t), \end{aligned} \tag{4}$$

where $u(t) = \bar{u}(t)$, $y(t) = \bar{y}(t)$, $e(t) = \bar{e}(t)$, and

$$\mathbf{A} = \begin{pmatrix} \bar{\mathbf{A}} & \mathbf{0} \\ -\bar{\mathbf{C}} & -\delta \end{pmatrix}, \tag{5}$$

$$\mathbf{B} = \left(\bar{\mathbf{B}}^T \quad 0\right)^T, \tag{6}$$

$$\mathbf{N} = \left(\mathbf{0}^T \quad 1\right)^T, \tag{7}$$

$$\mathbf{w}(t) = \left(\bar{\mathbf{w}}^T(t) \quad 0\right)^T, \tag{8}$$

$$\mathbf{C} = \left(\bar{\mathbf{C}} \quad 0\right). \tag{9}$$

C. Open-Loop Operation and Steady State Removal

When operated in open-loop, the system equations are valid around an operating point, here referred to as the steady state. When formulating the LQG problem for closed-loop operation, it is convenient to first remove the nonzero operating point from all signals, since LQG is typically formulated without consideration of biases. Assume that

A1) The constant operating point of the control system is defined by the steady state signal values y_s^{ref}, y_s, u_s and $\mathbf{x}_s$, where $y_s = \bar{y}_s$ and $u_s = \bar{u}_s$.

When used as a subscript, $_s$ thus denotes steady state. The use of integral control implies

$$y_s = y_s^{ref}. \tag{10}$$

Then, by the superposition principle, the zero mean disturbances $\mathbf{w}(t)$ and $e(t)$ are temporarily disregarded. By using (4) and the fact that in steady state $\dot{\mathbf{x}}(t) = 0$

$$0 = \bar{\mathbf{A}}\bar{\mathbf{x}}_s + \bar{\mathbf{B}}\bar{u}_s, \tag{11}$$

$$0 = -\bar{\mathbf{C}}\bar{\mathbf{x}}_s - \delta x_{n+1,s} + y_s^{ref} = -\bar{\mathbf{C}}\bar{\mathbf{x}}_s - \delta 0 + y_s^{ref}. \tag{12}$$

The last equality follows since (12) needs to be consistent with the measurement equation in steady state, cf. (1), (4), (9). Define the zero mean state, state estimate, input, output and reference signals

$$\tilde{\mathbf{x}}(t) = \mathbf{x}(t) - \mathbf{x}_s, \tag{13}$$

$$\hat{\tilde{\mathbf{x}}}(t) = \hat{\mathbf{x}}(t) - \mathbf{x}_s, \tag{14}$$

$$\tilde{u}(t) = u(t) - u_s, \tag{15}$$

$$\tilde{y}(t) = y(t) - y_s^{ref}, \tag{16}$$

$$\tilde{y}^{ref}(t) = y^{ref}(t) - y_s^{ref}. \tag{17}$$

Using the superposition principle again to bring back the disturbances, and using (3) - (9) and (13) then give

$$\begin{aligned}\dot{\tilde{\mathbf{x}}}(t) = \dot{\mathbf{x}}(t) &= \mathbf{A}\mathbf{x}(t) + \mathbf{B}u(t) + \mathbf{N}y^{ref}(t) + \mathbf{w}(t) \\ &= \mathbf{A}\tilde{\mathbf{x}}(t) + \mathbf{B}\tilde{u}(t) + \mathbf{N}\tilde{y}^{ref}(t) + \mathbf{w}(t) \\ &\quad + \mathbf{A}\mathbf{x}_s + \mathbf{B}u_s + \mathbf{N}y_s^{ref}. \end{aligned} \tag{18}$$

As may be readily checked using (3), (5)-(9), (11) and (12), the last three terms of (18) sum up to $\mathbf{0}$, i.e.

$$\dot{\tilde{\mathbf{x}}}(t) = \mathbf{A}\tilde{\mathbf{x}}(t) + \mathbf{B}\tilde{u}(t) + \mathbf{N}\tilde{y}^{ref}(t) + \mathbf{w}(t). \tag{19}$$

Similarly

$$\begin{aligned}\tilde{y}(t) = y(t) - y_s^{ref} &= \mathbf{C}\mathbf{x}(t) + e(t) - y_s^{ref} \\ &= \mathbf{C}\tilde{\mathbf{x}}(t) + e(t) + \bar{\mathbf{C}}\bar{\mathbf{x}}_s + \delta 0 - y_s^{ref}. \end{aligned} \tag{20}$$

The sum of the last three terms equals 0 by (12) and therefore

$$\tilde{y}(t) = \mathbf{C}\tilde{\mathbf{x}}(t) + e(t). \tag{21}$$

Finally, define the control objective as

$$\tilde{\mathbf{z}}(t) = \mathbf{z}(t) - \mathbf{z}_s = \begin{pmatrix} \bar{\mathbf{C}} & 0 \\ \mathbf{0}^T & 1 \end{pmatrix} \tilde{\mathbf{x}}(t) = \mathbf{M}\tilde{\mathbf{x}}(t). \tag{22}$$

The dynamics of (19) and (21) is now equivalent to (4), but with the steady state removed.

D. Linear Quadratic Gaussian Regulation

Assume that

A2) $\mathbf{w}(t)$ is Gaussian, zero mean with covariance matrix $\mathbf{R}_1 \geq \mathbf{0}$.
A3) $e(t)$ is Gaussian, zero mean with variance $R_2 > 0$.
A4) The pair $(\mathbf{A}, \mathbf{C})$ is detectable.
A5) The pair $(\mathbf{A}, \mathbf{R}_1)$ is stabilizable.
A6) The penalty matrix $\mathbf{Q}_1 \geq \mathbf{0}$.
A7) The penalty matrix $Q_2 > 0$.
A8) The pair $(\mathbf{A}, \mathbf{B})$ is stabilizable.
A9) The pair $(\mathbf{A}, \mathbf{M^T Q_1 M})$ is detectable.

The above conditions lead to the following standard result, where E denotes expectation:

Lemma 1 (LQG control, [2], Theorem 5.4, Theorem 9.1, and [17], p. 175): Consider the time-invariant system (19) and (21). Assume that A1-A9 hold and consider the control problem

$$\begin{aligned}\min_{\tilde{u}\in\mathcal{L}_2} E\int_0^\infty \Big(&\left(\tilde{\mathbf{z}}(t) - \mathbf{M}\tilde{\mathbf{x}}(t)\right)^T \mathbf{Q}_1 \left(\tilde{\mathbf{z}}(t) - \mathbf{M}\tilde{\mathbf{x}}(t)\right) \\ &+ \tilde{u}^T(t) Q_2 \tilde{u}(t)\Big)\, dt. \end{aligned} \tag{23}$$

Then the optimal controller is given by

$$\tilde{u}(t) = -\mathbf{L}\hat{\tilde{\mathbf{x}}}(t) + \mathbf{L}^{ref}\tilde{\mathbf{z}}(t). \tag{24}$$

Here

$$\mathbf{L} = Q_2^{-1}\mathbf{B}^T\mathbf{S} \tag{25}$$

where $\mathbf{S} = \mathbf{S}^T > \mathbf{0}$ is a unique solution to

$$\mathbf{A}^T\mathbf{S} + \mathbf{S}\mathbf{A} + \mathbf{M}^T\mathbf{Q}_1\mathbf{M} - \mathbf{S}\mathbf{B}Q_2^{-1}\mathbf{B}^T\mathbf{S} = \mathbf{0}, \tag{26}$$

while

$$\mathbf{L}^{ref} = -Q_2^{-1}\mathbf{B}^T\left(\mathbf{A}^T - \mathbf{S}\mathbf{B}Q_2^{-1}\mathbf{B}^T\right)^{-1}\mathbf{M}^T\mathbf{Q}_1. \tag{27}$$

Furthermore,

$$\dot{\hat{\tilde{\mathbf{x}}}} = \mathbf{A}\hat{\tilde{\mathbf{x}}}(t) + \mathbf{B}\tilde{u}(t) + \mathbf{N}\tilde{y}^{ref}(t) + \mathbf{K}\left(\tilde{y}(t) - \mathbf{C}\hat{\tilde{\mathbf{x}}}(t)\right), \tag{28}$$

where the Kalman gain

$$\mathbf{K} = \mathbf{P}\mathbf{C}^T R_2^{-1}, \tag{29}$$

and where $\mathbf{P} = \mathbf{P}^T > \mathbf{0}$ is a unique solution to

$$\mathbf{A}\mathbf{P} + \mathbf{P}\mathbf{A}^T + \mathbf{R}_1 - \mathbf{P}\mathbf{C}^T R_2^{-1}\mathbf{C}\mathbf{P} = \mathbf{0}. \qquad \square \tag{30}$$

E. Re-substitution of the Steady State

To complete the regulator design it remains to compute $u(t)$ and $\hat{\mathbf{x}}(t)$. Insertion of (13)-(17) in (28) gives

$$\begin{aligned}\dot{\hat{\mathbf{x}}}(t) &= \dot{\hat{\tilde{\mathbf{x}}}}(t) \\ &= \mathbf{A}\hat{\mathbf{x}}(t) + \mathbf{B}u(t) + \mathbf{N}y^{ref}(t) + \mathbf{K}\left(y(t) - \mathbf{C}\hat{\mathbf{x}}(t)\right) \\ &\quad - \mathbf{A}\mathbf{x}_s - \mathbf{B}u_s - \mathbf{N}y_s^{ref} - \mathbf{K}\left(y_s^{ref} - \mathbf{C}\mathbf{x}_s\right). \end{aligned} \tag{31}$$

Using the partitioning (5)-(9), together with (11) and (12), it is found that the last four terms sum up to zero. Hence

$$\dot{\hat{\mathbf{x}}}(t) = \mathbf{A}\hat{\mathbf{x}}(t) + \mathbf{B}u(t) + \mathbf{N}y^{ref}(t) + \mathbf{K}\left(y(t) - \mathbf{C}\hat{\mathbf{x}}(t)\right), \tag{32}$$

which appears in Fig. 1.

Referring to (15) and (24) the control signal becomes

$$\begin{aligned}u(t) &= u_s - \mathbf{L}\left(\hat{\mathbf{x}}(t) - \mathbf{x}_s\right) + \mathbf{L}^{ref}\left(\mathbf{z}(t) - \mathbf{z}_s\right) \\ &= -\mathbf{L}\hat{\mathbf{x}}(t) + \mathbf{L}^{ref}\mathbf{z}(t) + u_s + \mathbf{L}\mathbf{x}_s - \mathbf{L}^{ref}\mathbf{z}_s. \end{aligned} \tag{33}$$

Here the last three terms cancel by definition of the steady state applied to (24). It follows from (22) that

$$u(t) = -\mathbf{L}\hat{\mathbf{x}}(t) + L^{ref}y^{ref}(t). \tag{34}$$

III. FEEDBACK PATH DELAY INJECTION ATTACK

The objective of the attacker is to destabilize the closed-loop system, or achieving a significantly reduced damping as in [16]. It is assumed that the attacker has acquired access so that the control and feedback signals can be manipulated. Since the means of the attack is delay injection, input-output theory governs the effect on stability [3]. The definitions that underpin input-output stability theory can be found in the appendix. The appendix also states the Nyquist criterion which is used to prove the following elementary proposition that is exploited in sub-section V.C:

Proposition 1: Assume that the loop gain $\hat{g}(s)$ has order 2, is proper, minimum phase and stable with at most one pole in 0. Then the closed-loop system is $\mathcal{L}_2$-stable. $\square$

Proof: A calculation shows that $-\pi < Arg(\hat{g}(j\omega)) < \pi$. Hence the Nyquist plot is bounded away from the negative real axis and $-1 + j0$ is not encircled. $\square$

A. Delay Injection

1) Manipulation of time: In case time stamps are used, the attacker could manipulate the associated messages and, for example, decrease the time values of the control signal so that they appear to be earlier than they actually are. This way the system could be manipulated to delay the control action, thereby increasing the loop delay. Such actions could be introduced right after the controller implementation or just before the plant, as illustrated by Fig. 1. The same type of attack could also be applied in the feedback signal path, before or after the Kalman filter of Fig. 1.

2) Delayed signals: In case time stamps are not used, the attacker could instead delay the control signal message, either close to the control signal functionality or close to the plant, as illustrated in Fig. 1. The attacker may, for example, implement the attack by creating an additional queue in the signal path. The same type of attack could also be implemented in the feedback path, before or after the Kalman filter of Fig. 1.

B. Disguised Attack by Delay Injection Point Selection

There are several signal points of Fig. 1, where a delay attack could be attempted. An obvious question is then if there is a set of preferred delay injection points?

To answer the question, it is noted that the system is operating in either open-loop or closed-loop, as selected by the user. When the system is operated in open-loop an operator may then be able to detect the delay attack on the control signal path, by manually sensing the delayed response of the plant. This is particularly true in cases where a human closes the feedback loop. In a cruise control application the driver would, for example, be able to feel the slowed down response of the accelerator pedal command. Attacks on the control signal paths are therefore seldom perfectly disguised.

However, in case the delay attack is executed on the *feedback path*, no such open-loop control effect can be observed by a human operator that closes the feedback loop. On the contrary, a delay attack on the feedback path could be inserted and left dormant and *completely disguised* for as long as open-loop operation is maintained.

The conclusion is that the opportunities to disguise a delay injection attack are better if the attack targets the feedback path, rather than the control signal path. Even when the existing Kalman filter is used to monitor the system for anomalies, the delay attack induces a multiplicative anomaly that is difficult to detect without tailored approaches such as the one proposed later in this paper.

C. Destabilization

In any of the cases listed above, the delay starts affecting the stability (or damping) when the operation is switched from open-loop control to closed-loop control, since the loop gain $\hat{g}(s)$ corresponding to Fig. 1 is then modified to

$$\hat{g}_T(s) = e^{-sT}\hat{g}(s). \tag{35}$$

If in closed-loop when the attack is initiated, the destabilization or the reduced damping will be instantaneous.

IV. DELAY ATTACK DETECTION BY RECURSIVE IDENTIFICATION

The present paper proposes joint recursive identification of delay and dynamics to detect injected delays. The reason why recursive identification is preferred is that supervision and delay attack detection must be performed on line and in such situations recursive identification excels in terms of computational complexity, memory requirements and tracking ability [25]. The RPEM proposed for supervision and delay attack detection was introduced in [20], and it is of output error type. This is exactly the type of algorithm that was found to have the best performance in the evaluation of [9]. In the paper, the focus is on open-loop delay attack detection. The closed loop problem is significantly harder due to lack of signal excitation and is left for future research.

The algorithm of [20] jointly identifies the delay and dynamics of a continuous time nonlinear dynamic system in state space form. In the present paper scaling of the sampling period is applied as well, as explained in [26]. Next the model underpinning the RPEM algorithm is reviewed *in the setting with SISO linear dynamics* that is needed in the present paper.

A. Linear State Space Model With Delay

The model of [20] is an ordinary differential equation (ODE) in canonical state space form, with a single output delay. For time-invariant systems the delay location does not matter, hence the output delay can also model delays on the input side. It follows that a notation without bars is used, to remain consistent with [20] and Fig. 1. In section VII this is changed to a notation with bars, since then the open-loop plant without integrating control is identified.

1) Dynamic model: The input signal, state vector and output of the model are denoted by $u(t)$, $\hat{\mathbf{x}}(t,\boldsymbol{\theta}_S)$ and $\hat{y}(t,\theta_T,\boldsymbol{\theta}_S)$, respectively, where $\boldsymbol{\theta}_S$ is the parameter vector of the ODE and where $T=\theta_T$ is the delay parameter. The definition of these quantities and the system model are

$$\boldsymbol{\theta} = \begin{pmatrix}\theta_T & \boldsymbol{\theta}_S^T\end{pmatrix}^T, \tag{36}$$

$$\mathbf{u}(t) = \begin{pmatrix}u(t) & \dots & u^{(n-1)}(t)\end{pmatrix}^T, \tag{37}$$

$$\hat{\mathbf{x}}(t,\boldsymbol{\theta}_S) = \begin{pmatrix}\hat{x}_1(t,\boldsymbol{\theta}_S) & \dots & \hat{x}_n(t,\boldsymbol{\theta}_S)\end{pmatrix}^T, \tag{38}$$

$$\begin{aligned}&\dot{\hat{\mathbf{x}}}(t,\boldsymbol{\theta}_S)\\ &= \begin{pmatrix}\dot{\hat{x}}_1(t,\boldsymbol{\theta}_S)\\ \vdots \\ \dot{\hat{x}}_{n-1}(t,\boldsymbol{\theta}_S)\\ \dot{\hat{x}}_n(t,\boldsymbol{\theta}_S)\end{pmatrix} = \begin{pmatrix}\hat{x}_2(t,\boldsymbol{\theta}_S)\\ \vdots \\ \hat{x}_n(t,\boldsymbol{\theta}_S)\\ \boldsymbol{\varphi}^T\left(\hat{\mathbf{x}}(t,\boldsymbol{\theta}_S),u(t)\right)\boldsymbol{\theta}_S\end{pmatrix},\end{aligned} \tag{39}$$

$$\hat{\mathbf{y}}(t,\theta_T,\boldsymbol{\theta}_S) = \mathbf{C}\hat{\mathbf{x}}(t-\theta_T,\boldsymbol{\theta}_S) = \mathbf{C}\hat{\mathbf{x}}(t,\boldsymbol{\theta}). \tag{40}$$

Here $\mathbf{C}$ is the measurement matrix and $^{(i)}$ denotes differentiation i times. Referring to the parameter enumeration and corresponding nonlinear notation of [20], the regression and parameter vectors are given by

$$\boldsymbol{\theta}_S = \begin{pmatrix}\theta_{S,0\dots0} & \dots & \theta_{S,0\dots(n-1)} & \theta_{S,0\dots10} & \dots & \theta_{S,1\dots0}\end{pmatrix}^T, \tag{41}$$

$$\boldsymbol{\varphi}\left(\hat{\mathbf{x}}(t,\boldsymbol{\theta}_S),u(t)\right)=\Big(1\ \ ...\ \ u^{(n-1)}(t)$$

$$\hat{x}_n(t,\boldsymbol{\theta}_S)\ \ ...\ \ \hat{x}_1(t,\boldsymbol{\theta}_S)\Big)^T. \tag{42}$$

The notation may be unfamiliar when used for linear system, but it is needed to systemize the parameters of the multi-polynomial model of [20]. It is retained here to facilitate the use of the software [27]. To understand the notation it is useful to note that the parameter and regression vectors are filled with terms from left to right according to the indices of the parameter vector, where the outermost index varies the fastest. From left to right the indices represent the first state vector component to the last state vector component, with the rightmost index representing the input signal and its derivatives.

2) Delay model: The delay modeling allows identification of non-integer delays in terms of the sampling period T_S. The idea exploited in [20] is to interpolate between time shifted multiple state space models for identification of a fractional part of the delay. To do so the delay is parameterized by

$$\theta_T=T=mT_s+T_f,\quad m\in[0,M-1]. \tag{43}$$

Here m counts the number of sampling periods m of the delay, while T_f denotes the fractional delay such that,

$$0\leq T_f<T_S. \tag{44}$$

Then define $M+1$ models in terms of $u_m(t)$ and $\hat{\mathbf{x}}_m(t,\boldsymbol{\theta}_S)$,

$$u_m(t)=u(t-mT_S),\quad m=0,...,M, \tag{45}$$

$$\hat{\mathbf{x}}_m(t,\boldsymbol{\theta}_S)=\hat{\mathbf{x}}(t-mT_S,\boldsymbol{\theta}_S),\quad m=0,...,M. \tag{46}$$

Time invariance implies that (46) can be generated using the m:th delayed input of (39). In fact, these delayed states can be obtained by time shifting of previously generated states when the adaptation gain is small, thereby restricting the need for integration to one state ODE and one gradient ODE.

The RPEM interpolates inputs, state vectors and gradients, using the integer delay signals (45) and (46) *adjacent* to the running estimate of the delay. To define the interpolation mathematically, the running estimate of the delay, i.e. $\hat{\theta}_T(t)$ is first decomposed

$$\hat{\theta}_T(t)=\hat{m}(t)T_S+\hat{T}_f(t),\quad \hat{m}(t)\in[0,M-1]. \tag{47}$$

Linear interpolation then gives

$$\hat{\mathbf{x}}(t-\hat{\theta}_T(t),\hat{\boldsymbol{\theta}}_S(t))$$

$$=\left(1-\frac{\hat{T}_f(t)}{T_S}\right)\hat{\mathbf{x}}_{\hat{m}}(t,\hat{\boldsymbol{\theta}}_S(t))+\frac{\hat{T}_f(t)}{T_S}\hat{\mathbf{x}}_{\hat{m}+1}(t,\hat{\boldsymbol{\theta}}_S(t)). \tag{48}$$

The corresponding output signal becomes

$$\hat{\mathbf{y}}(t,\hat{\theta}_T(t),\hat{\boldsymbol{\theta}}_S(t))$$

$$=\hat{\mathbf{y}}(t-\hat{\theta}_T(t),\hat{\boldsymbol{\theta}}_S(t))=\mathbf{C}\hat{\mathbf{x}}(t-\hat{\theta}_T(t),\hat{\boldsymbol{\theta}}_S(t)). \tag{49}$$

B. The Recursive Prediction Error Method

To obtain the RPEM, a discretization of the continuous time state space model and gradient is performed with the Euler forward method. The discretization can exploit scaling of the actual sampling period, which has been found to enhance the performance of the algorithm significantly, see [26]. Such scaling is used in the present paper. Since output error identification is applied it is also necessary to check model stability online. This is done by a projection algorithm that maintains the parameters in the set of asymptotically stable models [20], [25]. The Gauss-Newton RPEM minimizes

$$V(\boldsymbol{\theta},\Lambda)=\frac{1}{2}\lim_{t\to\infty}E\left[\Lambda^{-1}(t,\boldsymbol{\theta})\varepsilon^2(t,\boldsymbol{\theta})+\ln\left(\Lambda(t,\boldsymbol{\theta})\right)\right], \tag{50}$$

using three recursive equations for the running estimate of the parameter vector $\hat{\boldsymbol{\theta}}(t)$, the Hessian $\mathbf{R}(t)$, and the estimated covariance matrix $\Lambda(t)$ of the prediction error $\varepsilon(t)$. Here

$$\varepsilon(t)=y(t)-\hat{y}(t,\hat{\theta}_T(t),\hat{\boldsymbol{\theta}}_S(t)), \tag{51}$$

where $y(t)$ is the measured output signal. The complete algorithm is listed in [20].

V. FEEDBACK PATH DELAY ATTACKS IN CRUISE CONTROL

Automotive cruise control is a well known application where the driver switches between open-loop and closed-loop operation, cf. [24] and [18]. Here the focus will be on the basic constant velocity regulation mode.

A. Linearized Dynamic Model

A vehicle cruising at a speed $\bar{x}_1(t)$ is mainly affected by a forward force $m\bar{u}(t)$ where m is the mass of the vehicle and $\bar{u}(t)$ is the control signal commanded by the accelerator pedal or the cruise control system, and by a wind resistance force proportional to the square of the speed [19], [24]. When linearized the wind resistance may be written as $-\gamma\bar{x}_1(t)$. The vehicle is also affected by a deterministic disturbance force $-m\bar{d}(t)$ caused by the varying vertical slope of the road [19]. No measurement is assumed to be available for $\bar{d}(t)$. Other friction forces are also present [19], however for the purpose of the paper, the following model that result from Newton's second law is sufficient

$$\dot{\bar{x}}_1=-\frac{\gamma}{m}\bar{x}_1(t)+\bar{u}(t)-\bar{d}(t). \tag{52}$$

The speed can, for excample, be measured with GPS, i.e.

$$\bar{y}(t)=\bar{x}_1(t)+\bar{e}(t), \tag{53}$$

where $e(t)$ is a small measurement disturbance.

B. Linear Quadratic Integrating Regulator

Since the main system disturbance $-\bar{d}(t)$ is not random, and since GPS provides very accurate speed measurements, the controller design is here relaxed from LQG control to LQ-control, by disregarding the Kalman filter of Lemma 1.

Proceeding with controller design using Lemma 1, it follows from (52) and (53) that $\bar{\mathbf{A}}=-\gamma/m$, $\bar{\mathbf{B}}=1$ and

$\bar{\mathbf{C}} = 1$. The input signal penalty is given by $Q_2 = q_2$, while a diagonal state penalty matrix is selected, i.e.

$$\mathbf{Q}_1 = \begin{pmatrix} q_{11} & 0 \\ 0 & q_{22} \end{pmatrix}. \tag{54}$$

Then, since $\mathbf{M} = \mathbf{I}_2$ is the unity matrix, (5), (6) and the Riccati equation (26), give

$$\frac{1}{q_2}s_{11}^2 + 2\frac{\gamma}{m}s_{11} + 2s_{12} - q_{11} = 0, \tag{55}$$

$$\frac{\gamma}{m}s_{12} + \frac{1}{q_2}s_{11}s_{12} + s_{22} = 0, \tag{56}$$

$$\frac{1}{q_2}s_{12}^2 - q_{22} = 0. \tag{57}$$

The positive definite analytical solution to (26) is obtained (in order) from

$$s_{12} = -\sqrt{q_{22}q_2}, \tag{58}$$

$$s_{11} = -\frac{\gamma q_2}{m} + \sqrt{\frac{\gamma^2 q_2^2}{m^2} + q_2 q_{11} - 2q_2 s_{12}}, \tag{59}$$

$$s_{22} = -\frac{\gamma}{m}s_{12} - \frac{1}{q_2}s_{11}s_{12}. \tag{60}$$

The controller gains are obtained from (25) and (27) as

$$\mathbf{L} = \begin{pmatrix} L_1 & L_2 \end{pmatrix} = \frac{1}{q_2}\begin{pmatrix} s_{11} & s_{12} \end{pmatrix}. \tag{61}$$

With $\mathbf{S}$ available, straightforward algebra gives

$$\mathbf{L}^{ref} = \frac{1}{q_2}\left(\frac{q_{11}}{\frac{\gamma}{m} + \frac{s_{11}}{q_2}} \quad -\frac{1}{\delta}\frac{q_{22}}{\frac{\gamma}{m} + \frac{s_{11}}{q_2}} \right). \tag{62}$$

It follows from (22) and (34) that the terms of $\bar{u}(t)$ are

$$\bar{u}(t) = u(t)$$

$$= -\mathbf{L}\hat{\mathbf{x}}(t) + \frac{1}{q_2}\frac{q_{11}}{\frac{\gamma}{m} + \frac{s_{11}}{q_2}}y^{ref}(t) = -\mathbf{L}\hat{\mathbf{x}}(t) + L^{ref}y^{ref}(t). \tag{63}$$

as stated in Remark 1 and appearing in Fig. 1.

C. Transformation to the Frequency Domain

Since LQ control is applied, the state estimate of Lemma 1 is replaced by the state, resulting in the control signal

$$\bar{u}(t) = u(t) = -L_1 x_1(t) - L_2 x_2(t) + L^{ref}y^{ref}(t)$$

$$= L_1\left(y^{ref}(t) - x_1(t)\right) - L_2\int\left(y^{ref}(t) - x_1(t)\right)dt$$

$$+ \left(L^{ref} - L_1\right)y^{ref}(t)$$

$$= L_1\epsilon(t) - L_2\int\epsilon(t)dt + \left(L^{ref} - L_1\right)y^{ref}(t). \tag{64}$$

Here $\epsilon(t)$ is the control error. The transfer function $C(s)$ of the controller therefore becomes

$$C(s) = \left(L_1 - \frac{L_2}{s}\right) = \frac{L_1 s - L_2}{s}, \tag{65}$$

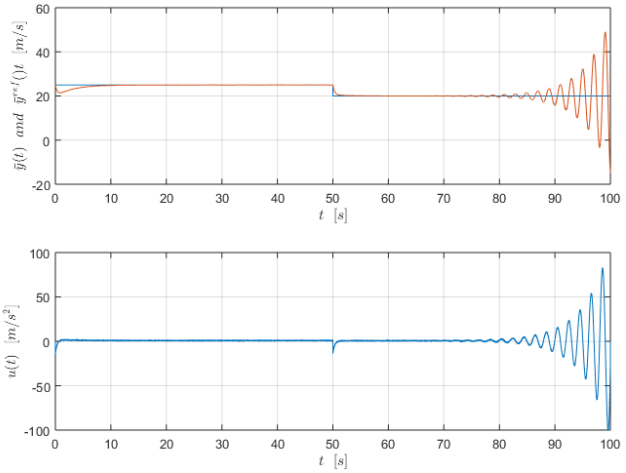

Fig. 2. Delay attack during closed-loop operation. Reference speed (blue) and cruise controlled speed (red) (top). Cruise control acceleration signal (bottom).

which represents PI-control, [28]. Using (52) and (53) gives the plant transfer function

$$H(s) = \frac{1}{s + \frac{\gamma}{m}}. \tag{66}$$

The loop gain therefore becomes

$$\hat{g}(s) = C(s)H(s) = \frac{L_1 s - L_2}{s\left(s + \frac{\gamma}{m}\right)}. \tag{67}$$

It follows from (58) and (61) that $L_2 < 0$, and from (59) and (61) that $L_1 > 0$. Hence the loop gain is minimum phase. Since the order is 2, the loop gain is (strictly) proper, there is one pole in 0 and one asymptotically stable pole, it follows from Proposition 1 that the closed-loop system is $\mathcal{L}_2$-stable. Note that this is true for all controllers with these properties, not only LQ control which can be proved to give a stable closed-loop system by other methods.

D. Destabilization by Feedback Path Delay Injection

The attack destabilizes the system by injection of delay in the feedback path, which modifies the loop gain of (67) by a phase loss according to

$$\hat{g}_T(s) = e^{-sT}\frac{L_1 s - L_2}{s\left(s + \frac{\gamma}{m}\right)}. \tag{68}$$

To illustrate the effect of a delay attack, vehicle movement was simulated with closed-loop cruise control using the parameters $\gamma = 50\ Ns/m$, $m = 1500\ kg$. The standard deviation of $\bar{e}(t)$ was $0.1\ m/s$. The control signal penalty was $q_2 = 1.00$, while the state penalties where $q_{11} = 10.00$ and $q_{22} = 1.00$, respectively, emphasizing integral control. Tustin's approximation, [29] was used to discretize the system with a sampling period of $T_s = 0.001\ s$. The system was simulated for $100\ s$, with a delay attack occurring after $65\ s$ injecting a delay of $T = 0.50\ s$. As is evident from Fig. 2 the instability becomes increasingly troublesome for the driver.

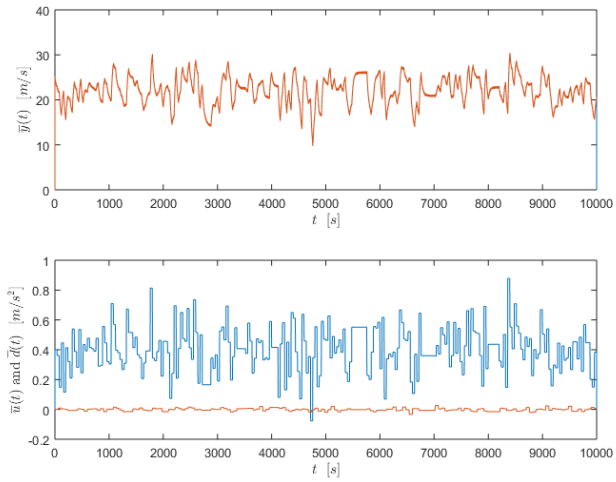

Fig. 3. Delay attack at $t = 4000$ s during open-loop operation. Speed (top), accelerator control signal (blue) and disturbance red (bottom).

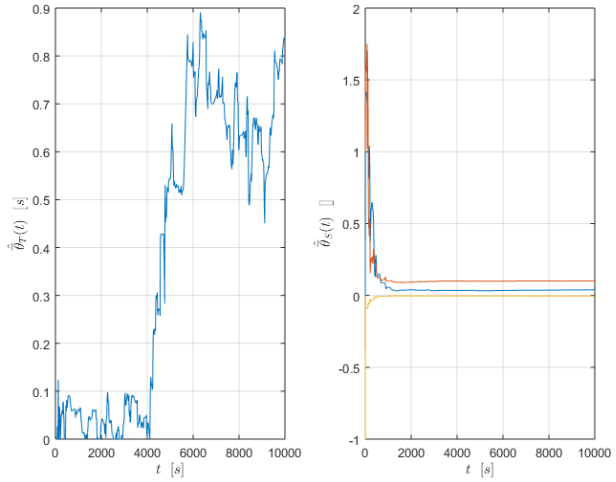

Fig. 4. Detection of delay attack during open-loop operation. Recursively identified delay parameter (left), recursively identified parameters of the vehicle dynamics (right).

VI. DELAY ATTACK DETECTION IN CRUISE CONTROL

A. Linear Dynamic Model With Delay

The RPEM described in Section V is the basis for the delay attack detection and the focus here is on the performance of this identification algorithm. A complete automated delay attack detection algorithm requires safety nets and additional logic that is beyond the scope of the present paper.

The RPEM is used to recursively identify the dynamics and the delay between the signal point where the open-loop accelerator input signal $\bar{u}(t)$ enters in Fig. 1, to the measured output speed, at the closed/open-loop switch. The dynamic model of this path is assumed to be given by

$$\dot{\hat{\bar{x}}}_1(t, \bar{\boldsymbol{\theta}}_S) = \hat{\bar{\theta}}_{S,00}(t)1 + \hat{\bar{\theta}}_{S,01}(t)\bar{u}(t) + \hat{\bar{\theta}}_{S,10}\hat{\bar{x}}_1(t, \hat{\bar{\boldsymbol{\theta}}}_S(t)), \tag{69}$$

$$\hat{\bar{y}}(t, \hat{\bar{\theta}}_T(t), \hat{\bar{\boldsymbol{\theta}}}_S(t)) = \hat{\bar{x}}_1(t - \hat{\bar{\theta}}_T(t), \hat{\bar{\boldsymbol{\theta}}}_S(t)). \tag{70}$$

$\hat{\theta}_{S,00}(t)$ is included to compensate for acceleration bias.

B. Delay Detection in Open-Loop

The numerical values of subsection VI.D were used for data generation. The driver accelerator signal $\bar{u}(t)$ was generated as a uniform Gaussian process, with mean 0.40 m/s^2, standard deviation 0.15 m/s^2, switching every 40 s. The disturbance $\bar{d}(t)$ was also generated as a Gaussian random process with mean 0.0 m/s^2, standard deviation 0.01 m/s^2, switching every 60 s. The delay attack appeared at time $t = 4000$ s, with injection of $T = 0.5$ s in the feedback path. The signals, sampled with $T_s = 0.10$ s for recursive identification appear in Fig. 3.

The RPEM was setup using sampling period scaling with a scale factor of $\alpha = 10$, cf. [20], [27]. The projection algorithm used a discrete pole radius of 0.9995, together with $M = 10$, i.e. the delay range was $[0.0\ s, 1.0\ s]$. The algorithm was tuned with an initial Hessian of $0.10I$ for the dynamics and 0.01 for the unknown delay. $\Lambda(0) = 1.0$ was used and the forgetting factor was 0.9999. The initial parameter vector was $\hat{\bar{\theta}}(0) = (0.000 \quad 0.000 \quad 1.000 \quad -1.000)^T$. The results of Fig. 4 shows that the algorithm converges quickly to a setting with $\hat{\bar{\theta}}_T(t) \approx 0.0$ s, where it remains until the delay attack. Immediately after the attack, $\hat{\bar{\theta}}_T(t)$ begins to increase toward the attack value $T = 0.5$ s , which is reached before $t = 5000$ s. Visual inspection indicates that an attack detection should be possible within 100 s after he attack, despite the fact that the attack appears to be completely disguised in Fig. 3. The value of the *re-scaled* [26] dynamic part of the parameter vector at the end of the run was

$$\hat{\bar{\boldsymbol{\theta}}}_S(10000) = (0.385 \quad 1.004 \quad -0.0036)^T \tag{71}$$

which is in good agreement with the values calculated from subsection VI.D

$$\bar{\boldsymbol{\theta}}_S^0 = (0.000 \quad 1.000 \quad -0.0033)^T. \tag{72}$$

VII. CONCLUSIONS

The paper discussed cyber attacks on feedback loops by injection of delay, with the purpose of destabilization. In case the system is operated in both open-loop and closed-loop it was shown that it is advantageous for the attacker to inject delay in the feedback paths since then the attack remains disguised until closed-loop operation is initiated. Such cases include automotive cruise control which was used in the paper to illustrate a disguised attack together with a new supervision and attack detection method using joint recursive identification of the open-loop dynamics and the delay. The RPEM was shown to successfully and very rapidly detect the disguised delay attack.

Future work needs to focus on closed-loop detection of delay attacks that reduce damping but do not destabilize. This is a hard problem since the regulation objective is contradictory to the need for signal excitation for recursive identification. Further work on nonlinear ACC systems and platooning of vehicles are other interesting topics , [30], [31].

APPENDIX

$\mathcal{L}_p$ Stability Definitions

D1) For all $p \in [1, \infty)$, $\mathcal{L}_p[0, \infty)$ denotes the set of all measurable functions $f(\cdot) : [0, \infty) \to \mathcal{R}$, such that

$$\|f(\cdot)\|_p^p = \int_0^\infty |f(t)|^p dt < \infty.$$

D2) The set of all measurable functions $f(\cdot) : [0, \infty) \to \mathcal{R}$, such that their truncations

$$f_T(t) = \begin{cases} f(t), & 0 \le t \le T \\ 0, & t > T \end{cases} \in \mathcal{L}_p[0, \infty), \forall T,$$

is denoted the extension $\mathcal{L}_{pe}[0, \infty)$ of $\mathcal{L}_p[0, \infty)$.

D3) The mapping $A : \mathcal{L}_{pe} \to \mathcal{L}_{pe}$ is $\mathcal{L}_p$-stable if i) $Af \in \mathcal{L}_p$ whenever $f \in \mathcal{L}_p$, and ii) there exist finite constants l, c, such that

$$\|Af\|_p \le l\|f\|_p + c, \quad \forall f \in \mathcal{L}_p.$$

D4) $\mathcal{A}$ denotes the set of generalized functions of the form

$$f(t) = \begin{cases} 0, & t < 0 \\ \sum_{i=0}^\infty f_i \delta(t - t_i) + f_a(t), & t \ge 0 \end{cases},$$

where $\delta(\cdot)$ is the unit delta distribution, t_i are non-negative constant delays, $f_a(t)$ is measurable and

$$\sum_{i=0}^\infty |f_i| < \infty, \qquad \int_0^\infty |f_a(t)| dt < \infty.$$

D5) $\hat{\mathcal{A}}$ denotes the set of all function $\hat{f} : \mathcal{C}_+ \to \mathcal{C}$ that are Laplace transforms of elements of $\mathcal{A}$.

A system is hence $\mathcal{L}_p$-stable if the internal signals are all integrable using the $\mathcal{L}_p$-norm, provided that the external exciting signals are in $\mathcal{L}_p$, for some p.

The Nyquist criterion

Lemma 2 (Nyquist Criterion, [3] Theorem 6.6.58): Consider the system of Fig. 1 and denote its loop gain $\hat{g}(s)$. Assume that the inverse Laplace transform of the transfer function $\hat{g}(s)$ fulfils $g(\cdot) \in \mathcal{A}$. Then the system is $\mathcal{L}_2$-stable if and only if the Nyquist plot

$$\omega \in [0, \infty) \to Re[\hat{g}(j\omega)] + jIm[\hat{g}(j\omega)] \in \mathcal{C} \tag{73}$$

is bounded away from and does not encircle $-1 + j0$. □

REFERENCES

[1] E. Fridman, *Introduction to Time-Delay Systems: Analysis and Control*. Cham.: Springer, 2014.

[2] T. Glad and L. Ljung, *Control Theory - Multivariable and Nonlinear Methods*. London, UK: Taylor and Francis, 2000.

[3] M. Vidyasagar, *Nonlinear Systems Analysis*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1978.

[4] D. Kushner, "The real story of STUXNET", IEEE Spectrum, 2013.

[5] A. Chattopadhyay and U. Mitra, "Security against false data-injection attack in cyber-physical systems", *IEEE Trans. Contr. Network Systems*, vol. 7, no. 2, pp. 1015-1027, 2020.

[6] C. De Persis and P. Tesi, "Resilient Control under denial-of-service: results and research directions", *in R. M. Ferrari and A. M. H. Texeira (eds.), Safety Security and Privacy for Cyber-Physical Systems*, pp. 41-60, Cham. :Springer, 2021.

[7] H. Liu, Y. Mo and K. H. Johansson, "Active detection against replay attack: a survey on watermark design for cyber-physical systems", *in R. M. Ferrari and A. M. H. Texeira (eds.), Safety Security and Privacy for Cyber-Physical Systems*, pp. 145-171, Cham: Springer, 2021.

[8] M. S. Chong, H. Sandberg and A. M. H. Teixeira, "A tutorial introduction to security and privacy for cyber-physical systems", *Proc. European Control Conference*, Naples, Italy, 2019.

[9] S. Björklund and L. Ljung, "A review of time-delay estimation techniques", *Proc. 42nd IEEE Conference on Decision and Control*, pp. 2502-2507, Maui, Hawaii, USA, 2003.

[10] A. Sargolzaei, F. M. Segers, A. Abbaspour, C. D. Crane and W. E. Dixon, "Secure control design for networked control systems with nonlinear dynamics under time-delay-switch attacks", *IEEE Trans. Automat. Contr.*, vol. 68, no. 2, pp. 798-811, 2023.

[11] X.-C. Shanguan, Y. He, C.-K. Zhang, W. Yao, J. Liang and M. Wu, "Resilient load frequency control of power systems to compensate random time-delay attacks". *IEEE Trans. Ind. Elec.*, vol. 70, no. 5, pp. 5115-5128, 2023.

[12] K. S. Xiahou, Y. Liu and Q. H. Wu, "Robust load frequency control of power systems against random time-delay attacks", *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 909-911, 2021.

[13] G. Bianchin and F. Pasqualetti, "Time-Delay Attacks in Networked Systems", *in Ç. K. Koç (ed.), Cyber-Physical Systems Security*, pp. 157-174, Cham. :Springer, 2018.

[14] E. Korkmaz, A. Dolgikh, M. Davis and V. Skormin, "ICS security testbed with delay attack case study", *2016 Military Communications Conference*, pp. 283-288, 2016.

[15] M. Letourneau, G. Doyen, R. Cogranne and B. Matieau, "A comprehensive characterization of threats targeting low-latency services: the case of L4S", Preprint, in review.

[16] T. Wigren and A. Teixeira, "On-line identification of delay attacks in networked servo control", *Prep. 22nd IFAC World Congress*, pp. 1041-1047, Yokohama, Japan, July 9-14, 2023.

[17] A. E. Bryson and Y.-C. Ho, *Applied Optimal Control - Optimization, Estimation and Control*. New York, NY: Taylor and Francis, 1975.

[18] P. Nilsson, O. Hussien, A. Balkan, Y. Chen, A. D. Ames, J. W. Grizzle, N. Ozay, H. Peng and P. Tabuada, "Correct-by-construction adaptive cruise control: two approaches", *IEEE Trans. Contr. Systems Tech.*, vol. 24, no. 4, pp. 1294-1307, 2016.

[19] H. Yueming and L. Zhiyuan, "An $\mathcal{H}_2/\mathcal{H}_\infty$ robust control approach to electric vehicle constant speed cruise", *Proc. Chinese Control Conference*, pp. 2384-2389, July 22-24, Yantai, Chinam 2011.

[20] T. Wigren, "Networked and delayed recursive identification of nonlinear systems", *Proc 56th IEEE Conference on Decision and Control*, pp. 5851-5858, Melbourne, Victoria, Australia, 2017.

[21] H. Kurz and W. Goedecke, "Digital parameter-adaptive control of processes with unknown deadtime", *Automatica*, vol. 17, pp. 245-252, 1981.

[22] A. J. Isaksson, A. Horch and G. A. Dumondt, "Event-triggered deadtime estimation from closed-loop data", *Proc. American Control Conference*, pp. 3280-3285, Arlington, Virginia, USA, 2001.

[23] C. L. Nikias and R. Pan, "Time delay estimation in unknown Gaussian spatially correlated noise", *IEEE Trans. Speech, Signal Processing*, vol. 36, pp. 1706-1714, 1988.

[24] B. van Arem, C. J. G van Driel and R. Visser, "The impact of cooperative adaptive cruise control on traffic-flow scenarios", *IEEE Trans. Intelligent Transportation Systems*, vol 7, no. 4, pp. 429-436, 2006.

[25] L. Ljung and T. Söderström, *Theory and Practice of Recursive Identification*. Cambridge, MA: MIT Press, 1983.

[26] T. Wigren, "Scaling of the sampling period in nonlinear system identification", *Proc. American Control Conference*, pp. 5058-5065, Portland, Oregon, 2005.

[27] T. Wigren, "MATLAB software for nonlinear and delayed recursive identification - revision 2", Technical Reports from the Department of Information Technology, 2022-002, Uppsala University, Uppsala, Sweden, 2022.

[28] K.J. Åström and T. Hägglund, *Automatic Tuning of PID Controllers*. Research Triangle Park, NC: Instrument Society of America, 1988.

[29] A. V. Oppenheim and R. W. Schafer, *Digital Signal Processing*. Englewood Cliffs, NJ: Mc Graw Hill, 1975.

[30] H. K. Khalil, *Nonlinear Systems*. Upper Saddle River, NJ: Prentice Hall, 2002.

[31] R. H. Middleton and J. H. Braslavsky, "String instability in classes of linear time invariant formation control with limited communication range", *IEEE Trans. Automat. Contr.*, vol. 55, no. 7, pp. 1519-1530, 2010.