Delay attack and detection in cyber secure feedback control systems

Background

Cyber security is becoming an increasingly important aspect of feedback control systems, due to the accelerating automation over the internet of things (IoT). IoT creates new challenges by the opening of new wireless interfaces inside the feedback control loops. These new interfaces give attackers new opportunities. A typical wireless networked control system architecture is depicted in Fig. 1.

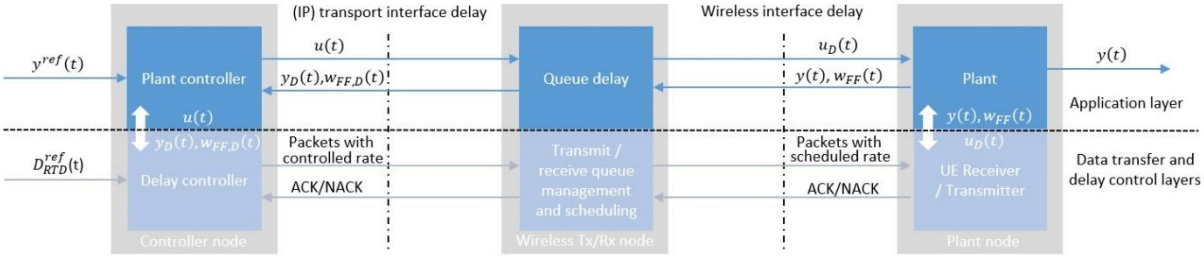

Figure 1. A wireless system architecture supporting networked feedback control.

Until recently, cyber security for feedback control systems have had to deal with conventional ways of attack, including deception, denial of service and replay. In addition, attackers have attempted to inject signals that are disguised by, for example, observability limitations in networked systems. In practice, attacks that focus on dynamic properties of systems have been very successful in the past, cf. the well-known STUXNET attack. There are however additional attack methods that can be used, but that have only been subject to a limited scientific discussion.

Delay Attack Objectives and Mechanisms

Delay is a main enemy of feedback control performance in general, it limits the achievable closed loop bandwidth and affects the possibilities of accurate regulation negatively, by limiting the low frequency gain, see e.g. 7. When applied to an existing feedback loop, the effects include delayed response, increased oscillation or ultimately destabilization.

This leads to the conclusion that delay attacks are relevant to achieve at least the following three objectives of an attacker:

- Response time violation. The objective of an attacker exploiting delay could be to introduce a response time delay, delaying downlink (DL) control actions. The effect aimed for could, for

example, be to make cascaded manufacturing stations of a production chain loose synchronization, thereby stopping or damaging the production chain, cf. 4.

- Settling time violation. The objective could be to reduce stability margins, thereby introducing overshoots and oscillation. This could be used to make the feedback loop under attack violate settling time requirements, such that a production process is stopped or the products or process itself are damaged. This is discussed further in the paper 4.
- Destabilization: The most dramatic objective of an attacker would be destabilization. As compared to the above objectives, more injected delay would be needed which is a disadvantage of this attack. Methods to disguise and detect such an attack are discussed in the papers 2, 3 and 4.

There are many attack mechanisms, among them a few that does not require the attacker to get access to the software systems implementing the feedback control loop. The most obvious method of this kind is

- Jamming. This method would use knowledge of the publicly standardized wireless signaling interfaces to apply selective jamming that delay DL control signals and /or uplink (UL) feedback and feedforward signals. Such delay could, for example, be introduced by retransmission of messages erased by the jamming. Many other possibilities exist. The attack could sometimes be disguised by internal or injected jitter, see Fig. 2.

Other types of attacks require access to the nodes hosting the SW systems in which the application control loops are implemented. They include

- Queue delay injection. This could be achieved by injection of fake packages into queues exploited by wireless transmission nodes and routers, see Fig.1.
- Time stamp manipulation. By manipulating the time stamps to represent an earlier time of transmission, any flow control mechanism as the one depicted in Fig. 1 could be made to increase the actual round trip delay (RTD). Manipulation of time stamps could also be useful to disguise other types of delay attacks.

A final consideration is where the additional delay is injected. As discussed in the papers 2 and 3, it is advantageous to use

- Delay injection in the feedback path. The reason why this is advantageous is that when the system is in open loop operation, the attack is perfectly disguised in terms of effect on the output signals. An automotive cruise controller is an example of such a system, that enters closed loop operation only when the driver initiates cruise control. Effect of such attacks are discussed in the papers 2 and 3.

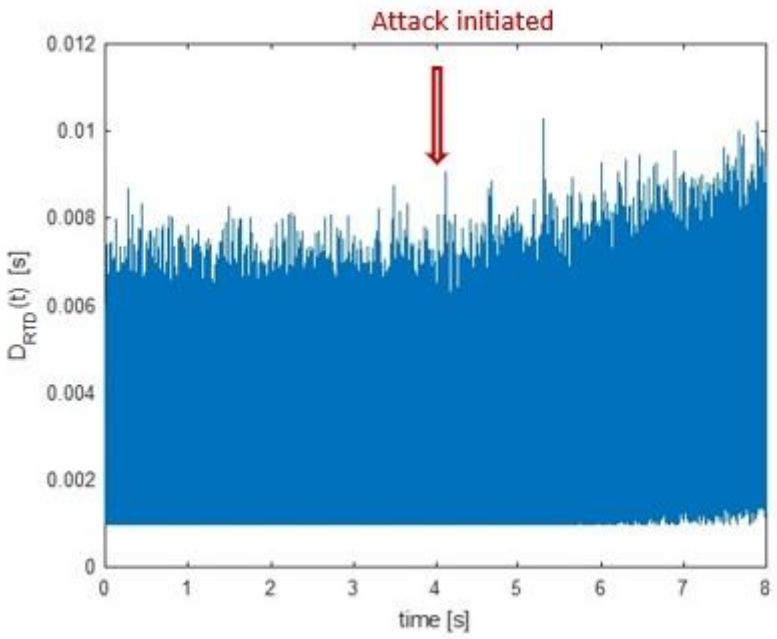

Figure 2. A delay attack on a PCB mounting station, disguised by jitter.

To illustrate the above discussion, and to show how delay attacks on servo control systems may be detected, the effect of the delay attack of Fig. 2 in terms of the settling time is explained in some detail. The attack is carried out against a tentative position servo control loop that positions a component mounting and soldering devise over a printed circuit board (PCB). A block diagram of the position control system is depicted in Fig. 3. The attack is carried out with a slowly increasing injected delay, here tentatively created by jamming and disguised by jitter, starting at time 4.000 s. The attack is not immediately visible in the RTD signal of Fig. 2. However, the effect on the settling time that is shown in Fig. 4 indicates a successful attack. Potentially, the attack could pass undetected unless more sensitive methods than visual inspection of the RTD are applied.

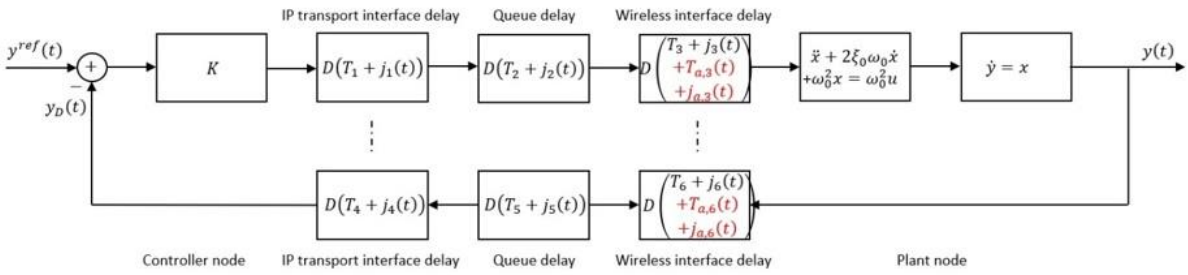

Figure 3. Block diagram of the position feedback loop of the PCB mounting machinery.

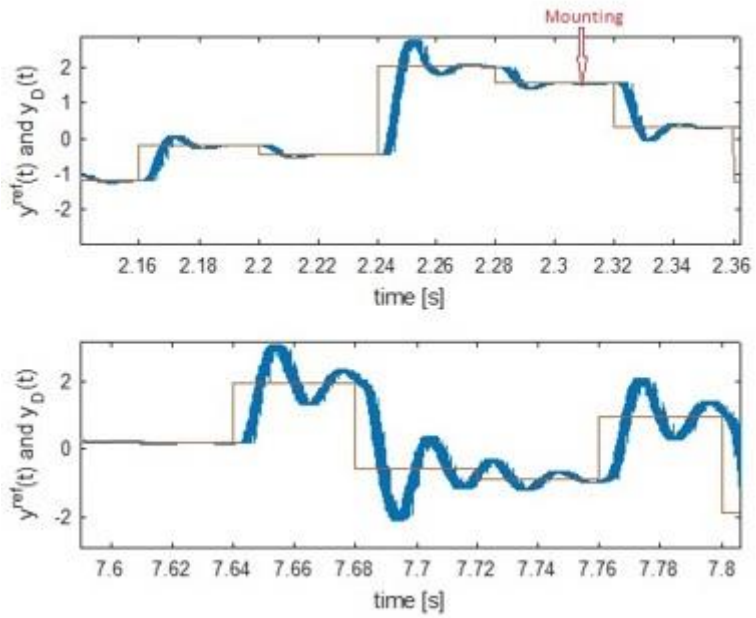

Figure 4. Step responses and settling time illustration without delay attack (top) and with delay attack (bottom). Note that mounting is scheduled within each step at the time indicated by the red arrow, clarifying the settling time violation

One way to detect a delay attack would be to identify (or equivalently, estimate) the delay online, followed by application of a change detection algorithm. A problem is then that the delay is produced as a part of a feedback control loop. This means that the performance of a pure delay identification scheme would be negatively affected by the processing of highly correlated signals, generated in closed loop.

For the above reason it is a better approach to perform joint recursive identification of the delay and the dynamics. Such estimation has been studied before, and it is known that so called output error based prediction error algorithms perform the best, see the papers 1, 2, 3, 4 for references. The papers 1 and 6 describes precisely such an algorithm, which is the reason why it is applied here. The algorithm can also use a scaling of the sampling period to improve the convergence properties, see 8. The algorithm is implemented in the software package 5, freely available for download and use. It can be noted that the dynamics that underpins the model of 6 is a general nonlinear ordinary differential equation in state space form, together with a polynomial parameterization. By restriction of parameters, it can also be used for modeling of purely linear dynamics. Finally, note that the paper 1 analyses the (global) convergence properties of the algorithm of 6. This analysis proves that the true parameter is in the set of global stationary points of the algorithm of 6. The scaling of 8 is accounted for by this analysis.

Since the position control system of the PCB mounting machinery above is a servo system, the closed loop system will be well excited by step responses, and will contain the RTD as a loop delay. It can therefore be expected that the approximate recursive prediction error algorithm of 6 will be able to successfully identify the delay and the dynamics. This is confirmed by Fig. 5 that depicts the time

evolution of the parameters of the dynamics together with the identified RTD. It can be seen that the RTD converges to closely resemble the true value of 1.00 ms during the first 3 seconds of the simulation. At the time the attack begins, the identified RTD starts to increase and a visual inspection of Fig. 5 indicates that a change detection scheme would be able to declare a delay attack well before time 5.0 s, perhaps as early as 0.5 s after the delay attack begins. It is noted that at this early stage, a visual inspection of Fig. 2 would not reveal an attack. It also needs to be noted that the RTD signal of Fig. 2 would need time stamps for its generation, something that an attacker may be able to manipulate as well. In such a situation, only the control- and output feedback signals of Fig. 6 would be available. However, no indication of a delay attack is clearly visible in these signals.

The recursive algorithm circumvents this by optimal processing of the reference and output signals, i.e. by recursive identification of the closed loop system.

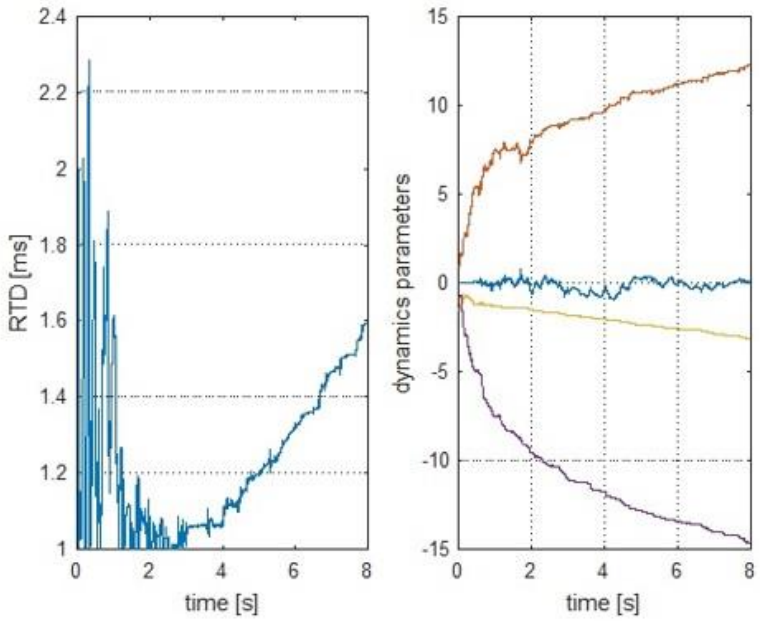

Figure 5. Estimated delay (left) and closed loop parameters of the dynamics (right).

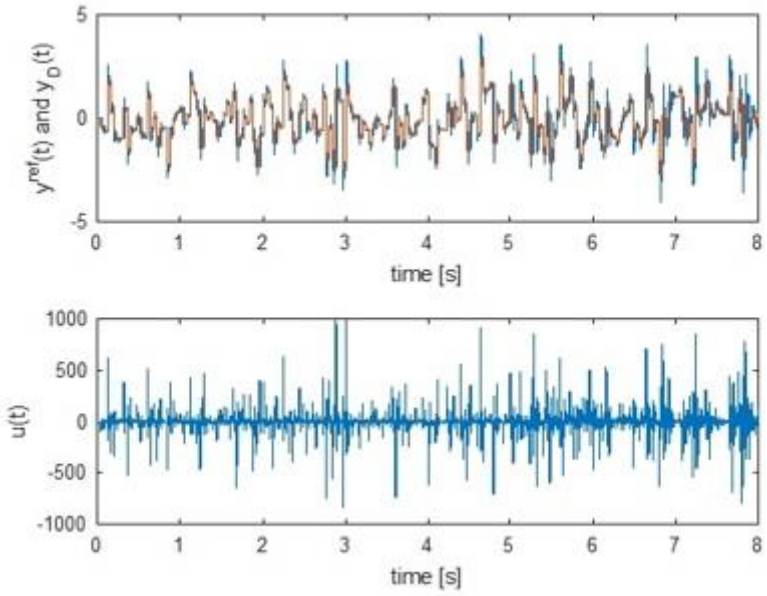

Figure 6. Control signal (bottom) and feedback signal (top).

Delay Attack and Detection on Feedback Regulator Loops

As compared to joint identification of delay and closed loop servo control dynamics, the identification of delay and dynamics for feedback regulators is more difficult. The main reason is that the regulation typically leads to poor excitation of the input and output signals used for identification. The difficulty increases when the system dynamics is nonlinear, as in 2.

In cases where the user closes the loop, a delay attack can be perfectly disguised in terms of the signals by performing the attack in the feedback path. In such a case the effect of the attack does not materialize until after the user closes the regulator loop. Fig. 7 depicts this situation.

To illustrate the effect of a delay attack, an automotive cruise control system was considered in the papers 2 and 3. The vehicle is mainly affected by forward thrust controlled by the driver via the accelerator pedal and air resistance proportional to the square of the relative air speed. In addition to terrain, wind gusts and friction affect the vehicle, however these forces can be neglected due to the application of integral control.

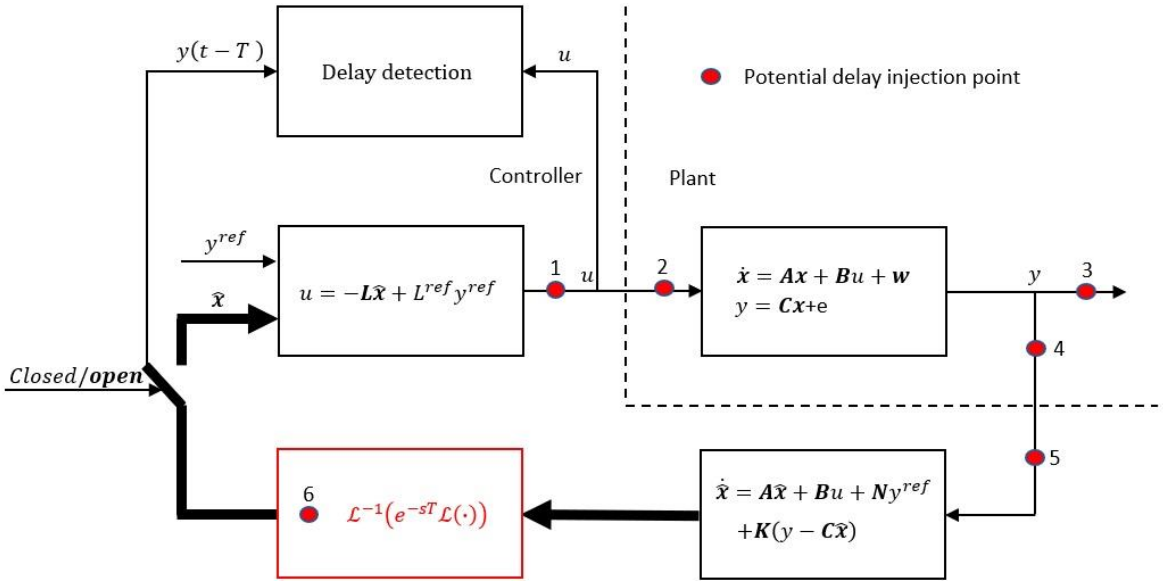

Figure 7. Block diagram of a manually closed feedback regulator loop. The red circles depict possible delay injection attack points, with the preferred point being no. 6.

The paper 3 considered a linear LQG based regulator design, based on a linearized version of the above Newtonian motion model. The effect of a delay injection attack during closed loop is illustrated in Fig. 8. The attack quickly becomes very disturbing for the driver. In the paper 2, the nonlinear Newtonian vehicle dynamics was instead considered, applying feedback linearization and constrained input control. The effect of the delay injection attack was equally disturbing, see 2 for details.

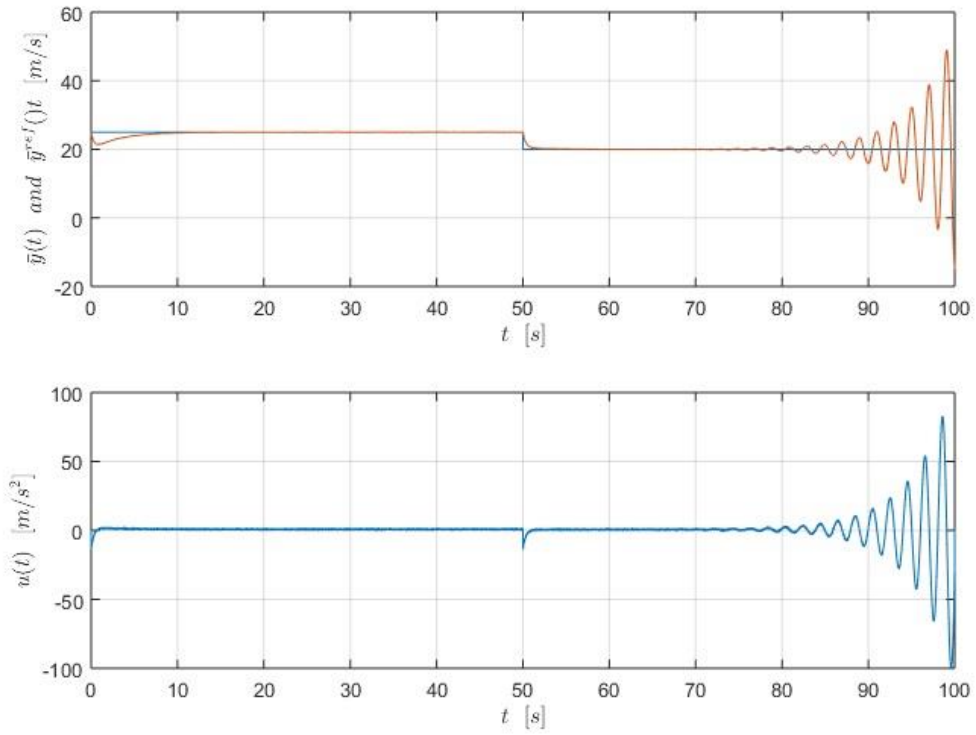

Figure 8. The effect on a delay attack on the linear cruise controller occurring at 65 seconds.

The algorithm of 6 that was analyzed in 1 was then applied for delay attack detection. The linearized cruise control system of 3 was operated in open loop, i.e. the attack occurring at time 4000 seconds was perfectly disguised as depicted in Fig. 9. As can be seen in Fig. 10 the attack is detected rapidly by the algorithm. Similar performance was obtained in 2, when applying the algorithm for joint identification of delay and nonlinear dynamics.

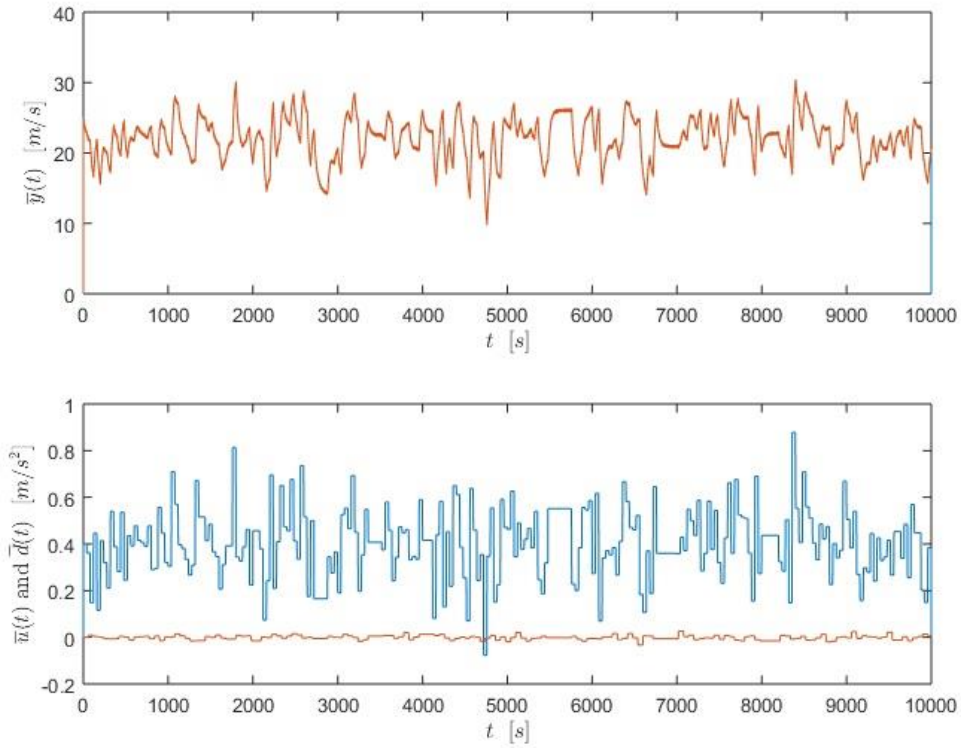

Figure 9. Control signal (left) and feedback signals in open loop (top).

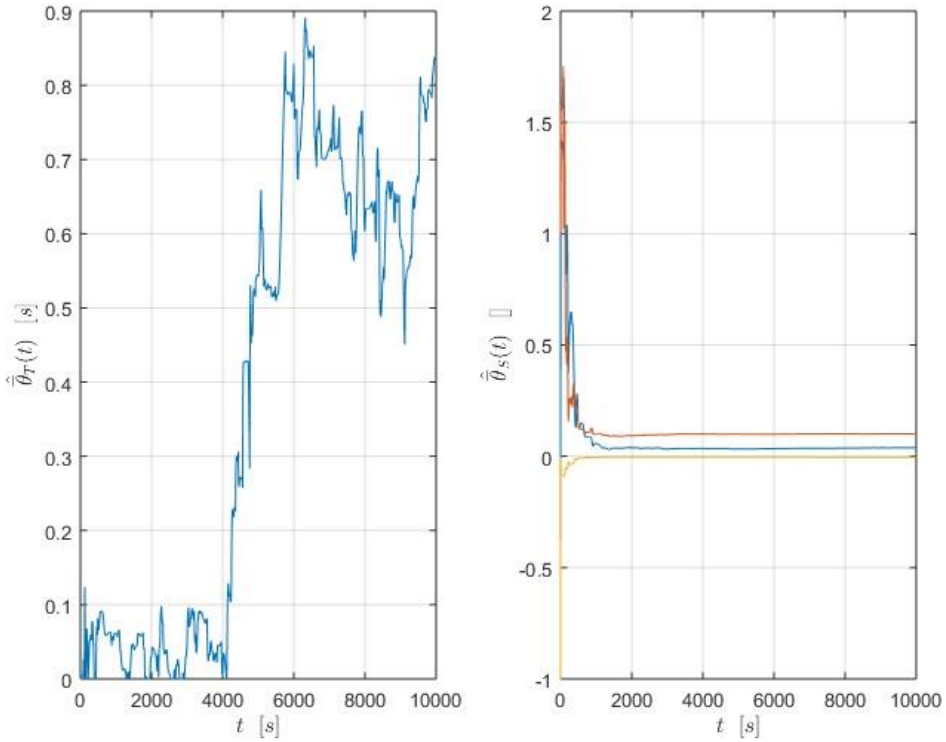

Figure 10. Estimated delay (left) and closed loop parameters of the dynamics (right).

References

1. T. Wigren, "Convergence in delayed recursive identification of nonlinear systems", Proc. European Control Conference, Stockholm, Sweden, June 25-28, pp. 914-921, 2024.

2. T. Wigren and A. Teixeira, "Delay attack and detection in feedback linearized control systems", Proc. European Control Conference, Stockholm, Sweden, June 25-28, pp. 1569-1576, 2024.

3. T. Wigren and A. Teixeira, “Feedback path delay attacks and detection”, in Proc. IEEE CDC, pp. 3864-3871, Singapore, December 13-15, 2023.

4. T. Wigren and A. Teixeira, “On-line identification of delay attacks in networked servo control”, IFAC World Congress, Yokohama, Japan, pp. 1041-1047, July 9-14, 2023.

5. 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, January, 2022.

6. T. Wigren, ``Networked and delayed recursive identification of nonlinear systems'',in Proc. IEEE CDC 2017, Melbourne, VA, Australia, pp. 5851-5858, Dec. 12-15, 2017.

7. T. Wigren, "Low frequency sensitivity function constraints for nonlinear L_2-stable networked control", Asian J. Contr., vol. 18, no. 4, pp. 1200-1218, 2016. DOI: 10.1002/asjc.1241.”

8. T. Wigren, ``Scaling of the sampling period in nonlinear system identification'', in Proc. ACC 2005, Portland, Oregon, U.S.A., pp. 5058--5065, June 8--10, 2005.