Secure Networked Motion Control Using Tampering Detection Observer

Jin Hoshino[1], Hitoshi Kojima[2], Takahiro Funakoshi[3], Ryusuke Imai[4], and Ryogo Kubo[5]
Department of Electronics and Electrical Engineering, Keio University
3–14–1 Hiyoshi, Kohoku-ku, Yokohama-shi, Kanagawa 223–8522, Japan
E-mail : [1]hoshino.jin@kbl.elec.keio.ac.jp, [2]kojima.hitoshi@kbl.elec.keio.ac.jp, [3]funakoshi.takahiro@kbl.elec.keio.ac.jp,
[4]imai.ryusuke@kbl.elec.keio.ac.jp, [5]kubo@elec.keio.ac.jp

Abstract: This paper proposes a tampering detection observer (TDO) to achieve safe and secure operation of a networked motion control system. The networked motion control system is comprised of a controller, communication networks with redundant feedback paths, and an electric motor. The proposed TDO detects tampering signals as an unexpected disturbance, and uses the redundant feedback paths to gain stable operations. Simulation results show that the proposed TDO can make it possible to keep stable operation of the networked motion control system with constant time delays even if tampering signals are injected on one of the feedback paths.

Keywords—**Networked Control System, Motion Control, Tampering, Cybersecurity, Time Delay**

1. Introduction

Motion control technologies in industrial fields, such as robotics and factory automation, have been rapidly developed [1]. Today, motion control technologies are also utilized in consumer electronics devices and electric vehicles, such as cars and planes, and not anymore rare in modern day life. In addition, along with the popularization of the Internet, control systems have been built over various kinds of communication networks. A networked control system (NCS) is one of the most attractive research topics in communication and control systems [2]. The stability and performance of the NCSs can deteriorate because of time delays, jitters, and information losses in the communication networks. We have studied time-delay and information-loss compensation techniques to improve the stability and performance in a networked motion control system [3], [4], [5]. In the previous studies, the time-delay and information-loss effects on the system were modeled as a network disturbance [6].

In recent years, there is a trend toward the increasing importance of cybersecurity in industrial control systems [7]. Cyberattacks to cause a decrease in confidentiality, integrity, and availability, e.g., tampering of control signals, are very critical in networked motion control. Since NCSs are utilized in many areas, losing the control of the NCSs can mean posing a risk to nations, economies and citizens [8]. The number of incidents in the NCSs has increased in the past years. Since 2005, car factories, pipe lines, and nuclear power plants have been recognized as targets of cyberattacks. Cars and planes have also become targets in the past few years [9]. The cyberattacks have spread out to other fields and are becoming a threat to our modern life.

Gaining a safe and secure NCS has become an urgent need, and there are many studies against the cyberattacks [10]. In the case of NCSs, the cybersecurity can be handled with information technology (IT) and network security [11]. However, the NCSs are built on Internet protocol (IP)-based networks, feedback loops, and coupling to physical environment, and therefore make it difficult to handle the security with only the IT and network security tools.

This paper proposes a tampering detection observer (TDO) to achieve safe and secure operation of a networked motion control system. The networked motion control system is comprised of a controller, communication networks with redundant feedback paths, and an electric motor. Tampering is one of the most critical cyberattacks in the NCSs. The proposed TDO detects tampering signals in networks as an unexpected disturbance and keeps stable operation of the networked motion control system with constant time delays. The validity of the proposed TDO in the networked motion control system is confirmed by simulation results.

This paper is organized as follows. The following section describes a conventional networked motion control system and a disturbance observer (DOB) for robust motion control. Section 3 proposes a tampering detection technique using the TDO. Simulation results are shown in Section 4. Finally, our conclusion is described in Section 5.

2. Networked Motion Control

This section presents a conventional networked motion control system with the robust acceleration control scheme using the DOB.

2.1 Conventional networked motion control

The block diagram of a networked motion control system is shown in Fig. 1. The system is comprised of a proportional and derivative (PD) controller, an electric motor, and network elements whose time delays are T_0 and T_1. The DOB is implemented to compensate load torque and achieve robust position control. In addition, x^{cmd}, x^{res}, x_d^{res}, u, u_d, and s denote the position command signal, position response signal, delayed position response signal, reference signal, delayed reference signal, and Laplace operator, respectively.

In the NCSs, the controller and plant are connected by the communication network. This enables the controller and plant to be separated physically, which improves the scalability of the system. By using the network, however, the time delays and packet losses are added to the reference and response signals. In addition, the conventional motion control system is vulnerable to the threat of tampering on the network because of the lack of a redundant path or a tampering detection technique.

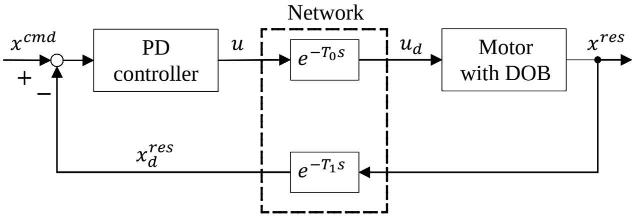
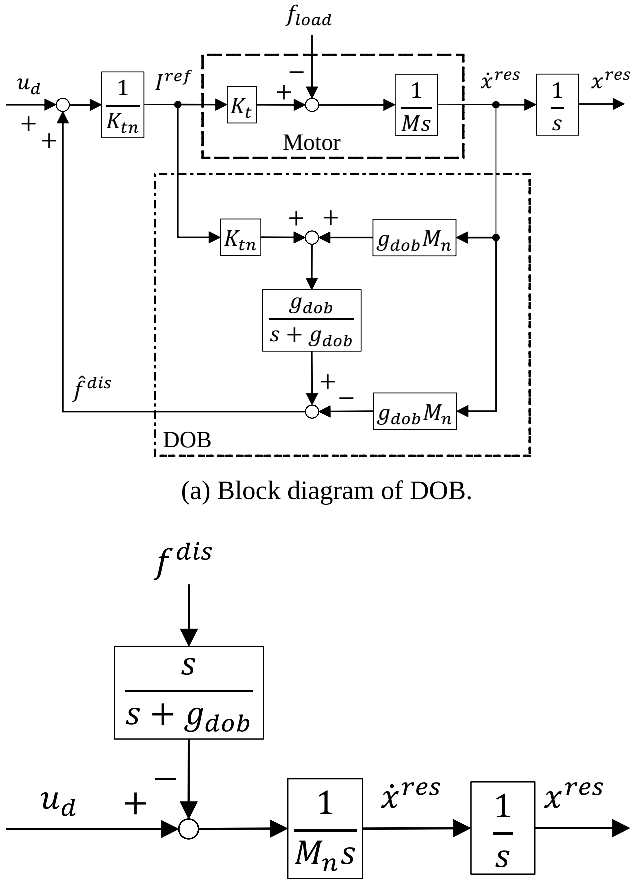


Figure 1. A networked motion control system.



(a) Block diagram of DOB.

(b) Equivalent system of Fig. 2(a).

Figure 2. DOB.

2.2 DOB

The block diagrams of the DOB and its equivalent system are shown in Fig. 2. In Fig. 2, f_{load}, M and K_t are the load torque, the moment of inertia, and torque constant, respectively. The subscript n stands for a nominal value.

The DOB estimates the disturbance as $\hat{f}^{dis}$. The disturbance force is estimated as (1) and (2)

$$\hat{f}^{dis} = \frac{g_{dob}}{s+g_{dob}} f^{dis}, \tag{1}$$

$$f^{dis} = f_{load} + \Delta M \ddot{x}^{res} + \Delta K_t I^{ref}, \tag{2}$$

where $\Delta M = M - M_n$ and $\Delta K = K_{tn} - K_t$, g_{dob} and I^{ref} are the cut-off frequency of a low-pass filter (LPF) and the reference current signal. Figure 2(a) can be transformed into Fig. 2(b). The disturbance f^{dis} is added to the system through a high-pass filter (HPF). When the cut-off frequency g_{dob} is high enough, f^{dis} is completely suppressed, and robust motion control is achieved.

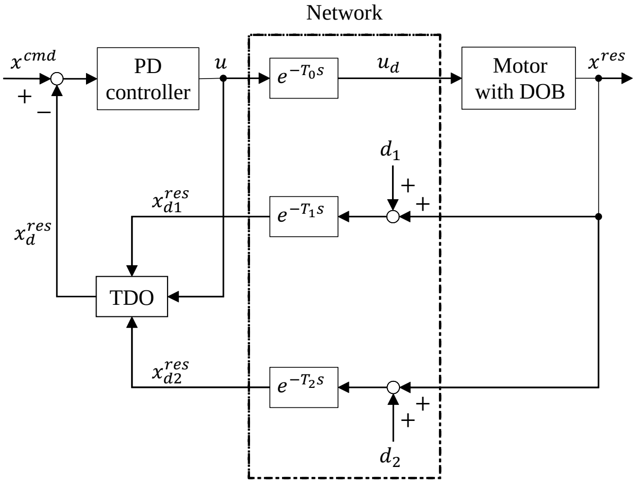


Figure 3. Networked motion control with TDO.

3. TDO-based Tampering Detection

This section proposes the TDO-based tampering detection technique for the networked motion control system.

3.1 Networked motion control with TDO

The block diagram of a networked motion control system with a tampering detection technique, i.e., the TDO, is shown in Fig. 3. The system includes the redundant feedback paths to cope with the injection of tampering signals on one of the feedback paths. In Fig. 3, x_{d1}^{res} and x_{d2}^{res} are the delayed response signals of feedback paths 1 and 2, respectively. In addition, T_1 and T_2 are time delays of the feedback paths, and d_1 and d_2 are unexpected disturbances or the models of tampering signals. In this research, tampering signals are injected on only one of the feedback paths with constant time delays, and the disturbance to the other path is assumed as zero.

3.2 Internal structure of TDO

The proposed TDO detects the tampering signals as a disturbance. The internal structure of the TDO is shown in Fig. 4. The reference signal u is input to the delay models of the redundant paths on the controller side. Then, the delayed reference signals $\hat{u}_{d1}$ and $\hat{u}_{d2}$ are input to the motor model which includes the DOB. After comparing the difference between x_{d1}^{res} and the estimated response signal for path 1 $\hat{x}_{d1}$ with the difference between x_{d2}^{res} and the estimated response signal for path 2 $\hat{x}_{d2}$, the selector selects the response signal used in the controller, x_d^{res}, as (3)

$$x_d^{res} = \begin{cases} x_{d1}^{res} & \text{if } |x_{d1}^{res} - \hat{x}_{d1}^{res}| < |x_{d2}^{res} - \hat{x}_{d2}^{res}| \\ x_{d2}^{res} & \text{if } |x_{d1}^{res} - \hat{x}_{d1}^{res}| \geq |x_{d2}^{res} - \hat{x}_{d2}^{res}| \end{cases}. \tag{3}$$

The path selection algorithm is summarized in Fig. 5.

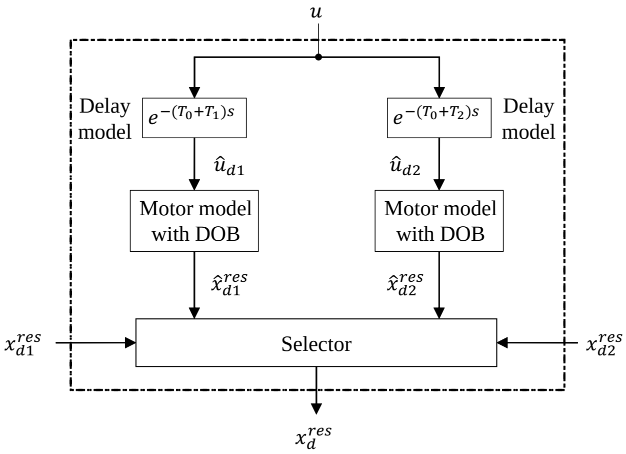


Figure 4. Internal structure of TDO.

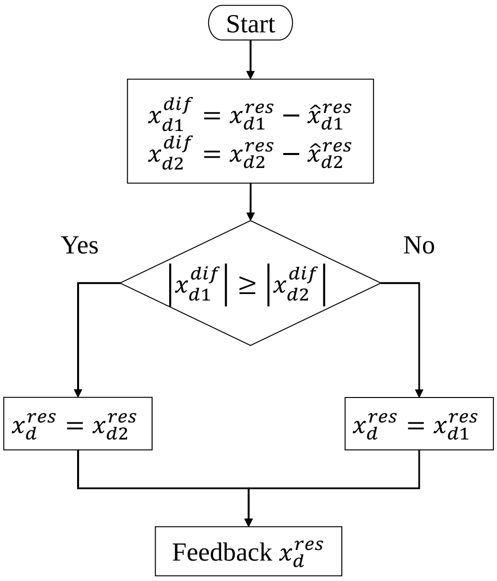

Start
$x_{d1}^{dif} = x_{d1}^{res} - \hat{x}_{d1}^{res}$
$x_{d2}^{dif} = x_{d2}^{res} - \hat{x}_{d2}^{res}$
Yes
No
$\left|x_{d1}^{dif}\right| \geq \left|x_{d2}^{dif}\right|$
$x_d^{res} = x_{d2}^{res}$
$x_d^{res} = x_{d1}^{res}$
Feedback x_d^{res}

Figure 5. Selector operation in TDO.

4. Simulation

This section shows the simulation results of the proposed TDO-based tampering detection technique and discusses the results.

4.1 Setup

Simulations were performed to confirm the validity of the proposed TDO. The simulations compared the conventional system without the TDO and the proposed system with the TDO. The transfer function of the PD controller G_c was set as (4)

$$G_c = 0.0166(400 + 40s). \tag{4}$$

The transfer function of the plant G_p was set as (5)

$$G_p = \frac{1.53}{0.0254s^2 + s}. \tag{5}$$

Table 1. Simulation parameters.

Cut-off frequency of pseudo-differential g_{pd}	100 rad/s
Cut-off frequency of DOB g_{dob}	100 rad/s
Time delay T_0	10 ms
Time delay T_1	10 ms
Time delay T_2	10 ms
Sampling period	1 ms

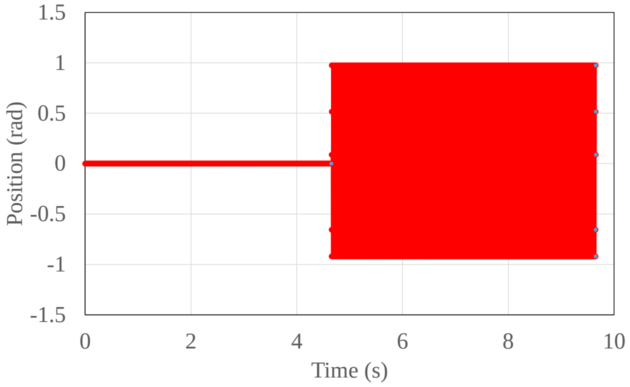


Figure 6. Injected tampering signal for path 2, d_2.

The other parameters for the simulations were set as Table 1. In the simulations, at 5 s, the tampering signal d_2 was injected on path 2 as an 800-Hz sinusoidal wave, while d_1 was not injected on path 1, as shown in Fig. 6.

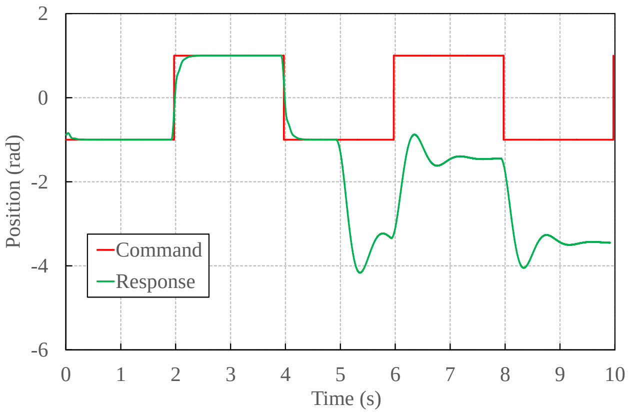
4.2 Results

The simulation results are shown in Fig. 7. As shown in Fig. 7(a), the position response could not be converged to the position command when the system did not include the TDO because of the injection of tampering signals. On the other hand, as shown in Fig. 7(b), the position response could be converged to the position command when the system included the TDO even if the tampering signals are injected on one of the feedback paths.

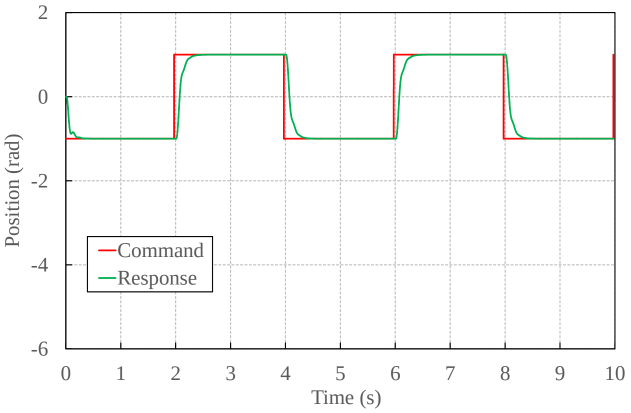
When the TDO did not detect any tampering signals, the feedback path was set to path 2, as shown in Fig. 8. On the other hand, at 5 s, the TDO detected tampering signals from the difference between $\hat{x}_{d2}^{res}$ and x_{d2}^{res}. The selector in the TDO changed the feedback path into path 1, since the difference between $\hat{x}_{d1}^{res}$ and x_{d1}^{res} was smaller than that of path 2. The simulation results showed that the TDO was able to offer a safe and secure networked motion control system by selecting a redundant path appropriately.

5. Conclusion

This paper proposed the TDO to achieve safe and secure operation of the networked motion control system. The simulation results showed that the proposed TDO could detect the tampering signals and select an appropriate feedback path. Our further studies include the consideration of time-varying delays and packet losses.



(a) Position control without TDO



(b) Position control with TDO

Figure 7. Simulation results.

Acknowledgment

This research was supported in part by JSPS KAKENHI Grant Number 16K16049, Kenjiro Takayanagi Foundation, and SECOM Science and Technology Foundation.

References

[1] K. Ohnishi, M. Shibata, and T. Murakami, "Motion control for advanced mechatronics," *IEEE/ASME Transactions on Mechatronics*, vol. 1, no. 1, pp. 56–67, Mar. 1996.

[2] R.A. Gupta and M.-Y. Chow, "Networked control system: Overview and research trends," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 7, pp. 2527–2535, July 2010.

[3] R. Kubo and K. Natori, "Dependable networked motion control using communication disturbance observer," *Proceeding of the 27th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2012)*, D-T1-05, pp. 1–4, July 2012.

[4] R. Imai and R. Kubo, "Introducing jitter buffers in networked control systems with communication disturbance observer under time-varying communication delays," *Proceedings of the 41st Annual Conference of the IEEE Industrial Electronics Society (IECON 2015)*, pp. 2956–2961, Nov. 2015.

[5] R. Imai and R. Kubo, "Experimental validation of communication disturbance observer for networked control systems with information losses," *IEICE Communications Express*, vol. 5, no. 4, pp. 102–107, Apr. 2016.

[6] K. Natori and K. Ohnishi, "A design method of communication disturbance observer for time delay compensation," *Proceedings of the 32nd Annual Conference of the IEEE Industrial Electronics Society (IECON 2006)*, pp. 730–735, Nov. 2006.

[7] NIST Special Publication 800-82, "Guide to industrial control systems (ICS) security," June 2011.

[8] S.M. Admin, and A.M. Giacomoni "Smart grid—safe, secure, self-Healing," *IEEE Power & Energy Magazine*, pp. 33–40, Jan./Feb. 2012.

[9] K. Koscher, A. Czeskis, F. Roesner, S. Patel, and T. Kohno, "Experimental security analysis of a modern automobile," *Proceeding of the 2010 IEEE Symposium on Security and Privacy (SP 2010)*, pp. 447–462, May 2010.

[10] H. Orjloo and M.A. Azgomi, "Evaluating the complexity and impacts of attacks on cyber-physical systems," *Proceedings of the CSI Symposium on Real-Time and Embedded Systems and Technologies (RTEST 2015)*, pp. 1–8, Oct. 2015.

[11] H. Sandberg, S. Amin, and K.H. Johansson, "Cyber-physical security in network control systems," *IEEE Control Systems Magazine*, pp. 20–23, Feb. 2015.

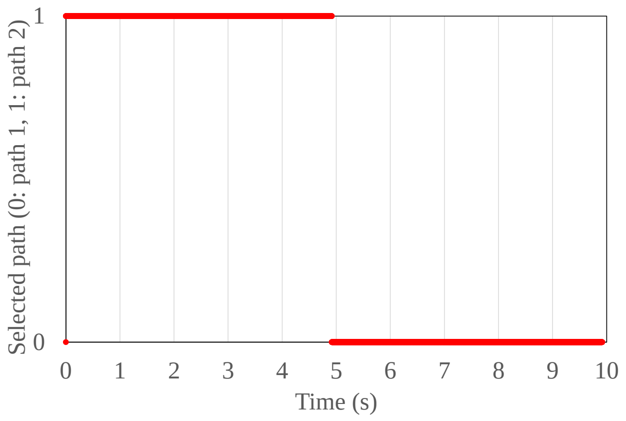


Figure 8. Path selected in the simulation using TDO.