2017 International Symposium on Nonlinear Theory and Its Applications,
NOLTA2017, Cancun, Mexico, December 4-7, 2017

A Tamper Detection Method Using Redundant Network Paths with Different Delays for Networked Control Systems

Kenta Yamada[1], Jin Hoshino[2], and Ryogo Kubo[3]

Department of Electronics and Electrical Engineering, Keio University
3–14–1 Hiyoshi, Kohoku-ku, Yokohama-shi, Kanagawa 223–8522, Japan
E-mail : [1]yamada.kenta@kbl.elec.keio.ac.jp, [2]hoshino.jin@kbl.elec.keio.ac.jp, [3]kubo@elec.keio.ac.jp

Abstract—There is a growing need for safe and secure networked motion control systems. This paper proposes a tamper detection method on a forward network path from a controller to an actuator. The proposed method utilizes a selector on the actuator side and redundant forward paths on which the same control signals are transmitted. In the selector, a correct signal is selected out of the received signals with or without tampering in consideration of different transmission delays on the redundant paths. The selector waits for receiving a control signal with the maximum transmission delay and compares the received signals transmitted at the same time. Experimental results using three forward paths show that the proposed method can achieve stable operation of the system even if one of the paths is tampered.

1. Introduction

The development of broadband communication networks is remarkable these days. This trend leads to a rapid development of motion control technologies such as robotics, factory automation [1]. These systems have been operated by remote control owing to the popularization of the Internet. Today, broadband communication using the Internet enables various kinds of devices with actuators controlled remotely. A remote control using the Internet can reduce capital expenditure (CAPEX) and operational expenditure (OPEX), and control with flexibility and high reliability [2]. The remote control systems using the Internet are called networked control systems (NCSs). The NCS is one of the most attractive research topics in the field of communications and control engineering [3].

While there are a lot of advantages in the NCSs, various kinds of factors which make the systems unstable exist in the NCSs. For example, there are unavoidable transmission delay, packet loss, quantization error in analog-to-digital conversion [4]. In addition, there exist not only these problems but also cyberattacks on the NCSs, because the Internet is not closed network [5]. According to increasing areas where the NCSs are utilized, attacking on the NCSs causes serious damages to nations, enterprises, and citizens [6]. The number of cyberattacks on the NCSs has increased in the past years. Car factories, pipe lines, and nuclear power plants have been regarded as targets for cyberattacks. These days, cars and airplanes have also become targets [7]. Therefore, spreading cyberattacks on the NCSs is becoming a threat to an individual life. Not to cause such a dangerous situation, making the NCSs safe and secure has become an urgent need, and a lot of studies are proposed against the cyberattacks [8].

A networked motion control system includes a controller, an electric motor as a plant, and communication networks. Tampering signal added in signals such as the control input and the plant output is one of the most critical cyberattacks in the NCSs. Muradore et al. [9] proposed the packet encryption method to achieve the secure NCS. Though the method can detect tampering and discard the tampered packets, the system cannot be controlled while the attacker tampers the packets. In addition, the tamper detection method using redundant feedback paths was proposed in [10]. The paper [10] detects tampering signal by comparing redundant feedback signals with output of a plant model. However, if the tampering signal is added in the forward path, the plant side cannot detect tampering because it is impossible to know what value is correct for the plant side.

This paper proposes a tamper detection method for forward paths to achieve safe and secure operation of a networked motion control system. The proposed method detects a tampered control signal by comparing the values received through the redundant forward paths without encryption. It maintains stable operation of the networked motion control system with constant transmission delays. Since redundant forward paths have different transmission delays, simply comparing the multiple signals which the plant receives at the same sampling time can not detect tampering. In the proposed method, the delayed time of multiple packets are adjusted virtually to compare the packets which sent at the same time. The validity of the proposed method in the networked motion control system is confirmed by experimental results.

This paper is organized as follows. Section 2 describes the NCS and a disturbance observer (DOB) for robust motion control. Section 3 proposes a tamper detection method to avoid using a tampered control signal. Experimental results are shown in Section 4. Finally, Section 5 concludes this paper.

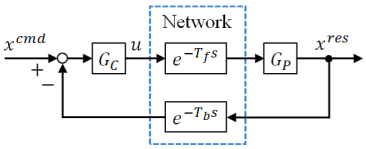

Figure 1: Block diagram of NCS

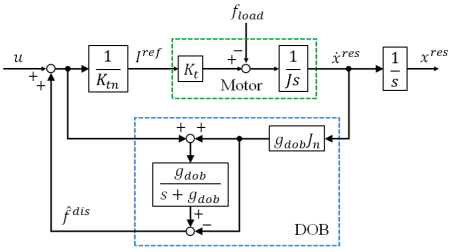

Figure 2: Block diagram of DOB

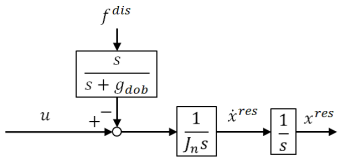

Figure 3: Equivalent system of Fig. 2

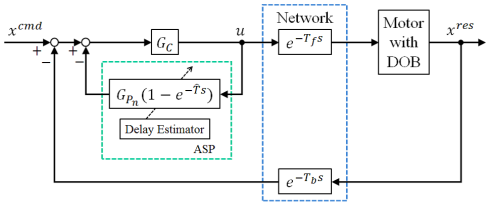

Figure 4: Block diagram of ASP

2. Networked Motion Control

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

2.1. NCS

Fig. 1 shows the block diagram of a networked motion control system. The communication network contains the forward and feedback transmission delays. In Fig. 1, x^{cmd}, x^{res}, u, T_f, T_b, and s are the position command signal, position response signal, control input signal, transmission delay on the forward path, transmission delay on the feedback path, and Laplace operator, respectively. The system includes a proportional-derivative (PD) controller G_C and an electric motor G_P.

In the NCSs, the packets exchanged between the controller and plant are transmitted through the communication network. Therefore, the stability and performance of the system are affected by the unavoidable transmission delay. In addition, the networked motion control system is defenseless against cyberattacks. It is important to take measures.

2.2. DOB

The DOB estimates the uncertainties and disturbances as a disturbance force $\hat{f}^{dis}$ as shown in Fig. 2. In Fig. 2, f_{load}, J, and K_t are the load force, the moment of inertia, and torque constant, respectively. The subscript n stands for a nominal value.

The disturbance force f^{dis} is estimated as (1) and (2)

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

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

where $\Delta J = J - J_n$ 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. Fig. 2 can be transformed into the equivalent system shown in Fig. 3. The disturbance force f^{dis} is input to the system through a high-pass filter (HPF) equivalently. If the cut-off frequency g_{dob} is large enough, the DOB suppresses the disturbance force, and robust motion control is achieved.

2.3. Adaptive Smith Predictor (ASP)

When the packets are transmitted through the network, there exists the unavoidable transmission delay. There are some transmission delay compensators such as the Smith predictor (SP), ASP, and communication disturbance observer (CDOB) [11]. Fig. 4 shows the block diagram of an NCS with the ASP. In Fig. 4, G_{P_n} and $\hat{T}$ are the nominal plant model and estimated round-trip time (RTT) model which equals the sum of T_f *and* T_b, respectively. Though the transfer function of the plant G_P is not equal to its model G_{P_n} actually, it assumed that the cut-off frequency of the HPF in the DOB is infinite and the plant can be transformed as G_{P_n} shown in Fig. 4. The delay estimator measures the RTT between the controller and plant by means of time stamp information of exchanged packets, and updates the RTT model. Therefore, the condition (3) is satisfied

$$\hat{T} = T. \tag{3}$$

The transfer function of the total control system is expressed as (4)

$$\frac{x^{res}}{x^{cmd}} = \frac{G_C G_{P_n} e^{-T_f s}}{1 + G_C G_{P_n}}. \tag{4}$$

3. Proposed Tamper Detection Method

This section proposes the tamper detection method for the networked motion control system.

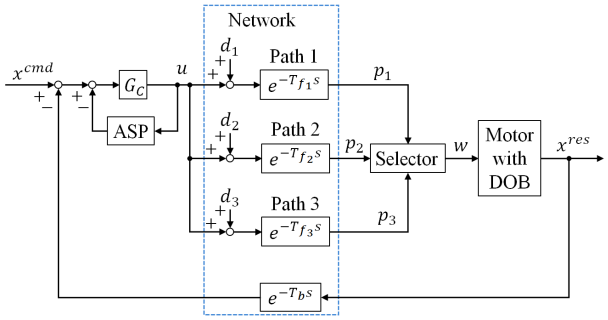

Figure 5: Block diagram of proposed method

Algorithm 1 Selection of control input w

$T_{max} = \max(T_{f_1},\ T_{f_2},\ T_{f_3})$
for $n = 1$ to 3 **do**
  $p'_{n,t_k} = p_{n,t_k - T_{max} + T_{fn}}$
end for
$A = |p'_{1,t_k} - p'_{2,t_k}|$
$B = |p'_{2,t_k} - p'_{3,t_k}|$
$C = |p'_{3,t_k} - p'_{1,t_k}|$
$M = \min(A,\ B,\ C)$
if $M == A$ **then**
  $w = p'_{1,t_k}$
else if $M == B$ **then**
  $w = p'_{2,t_k}$
else
  $w = p'_{3,t_k}$
end if

3.1. Packet Transmission Using Redundant Paths

The block diagram of proposed method is shown in Fig. 5. In Fig. 5, d_1, d_2, and d_3 denote unexpected disturbances or tampering signals added in forward path 1, 2, and 3, respectively, as shown in Fig. 6. In addition, T_{f_1}, T_{f_2}, and T_{f_3} are the transmission delays and p_1, p_2, and p_3 are the control inputs of forward path 1, 2, and 3, respectively, and w is the actual control input sent to the plant. This system includes the redundant three forward paths to compare the control input values and select the value considered to be correct.

3.2. Tamper Detection

On the plant side, it is impossible to know which control input is correct. As shown in Fig. 5, the plant side receives three packets p_1, p_2, and p_3 at each sampling time. p_{1,t_k}, p_{2,t_k} and p_{3,t_k} are the value of p_1, p_2, and p_3 which the plant side receives at the sampling time $t = t_k$ ($k = 1, 2, 3, ...$). The plant side can compare the values of these three packets sent at the same time, because these packets have time stamps. These packets should have the same values. If one of these packets has different value from the others, it is likely that the tampering signal is added to the value. This proposed algorithm is shown in Algorithm 1. In this paper, it is assumed that tampering signals are not added simultaneously in multiple paths, because this algorithm cannot detect tampering if the signals are added in majority paths.

Table 1: Parameters used in the experiments.

Cut-off frequency of pseudo-differential g_{pd}	100 rad/s
Cut-off frequency of DOB g_{dob}	100 rad/s
Transmission delay of forward path 1 T_{f_1}	10 ms
Transmission delay of forward path 2 T_{f_2}	25 ms
Transmission delay of forward path 3 T_{f_3}	40 ms
Transmission delay of feedback path T_b	10 ms
Sampling period	1 ms

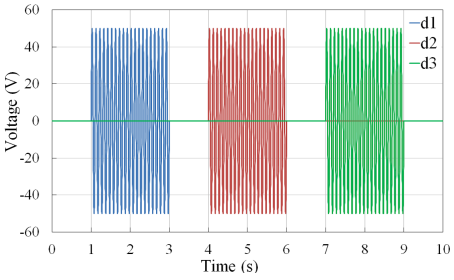

Figure 6: Injected tampering signals for the three paths

4. Experiment

This section shows the experimental results of the proposed method and discuss the results.

4.1. Setup

The experiments compared the conventional and proposed methods. It is assumed that conventional method has only one forward path and does not have any countermeasure against cyberattacks. The transfer function of the PD controller G_C was set as (5)

$$G_C = 0.0166(400 + 40s). \tag{5}$$

The transfer function of the nominal plant model G_{P_n} was set as (6)

$$G_{P_n} = \frac{1}{0.0166s^2}. \tag{6}$$

The parameters for the experiments were set as Table 1. Fig. 6 shows the tampering signals added to the three forward paths. These were the sinusoidal waves of a 50-V amplitude and a 10-Hz frequency. In the conventional method, only tampering signal d_1 was added in the forward path.

4.2. Results

The experimental results of the conventional and proposed methods are shown in Figs. 7 and 8, respectively.

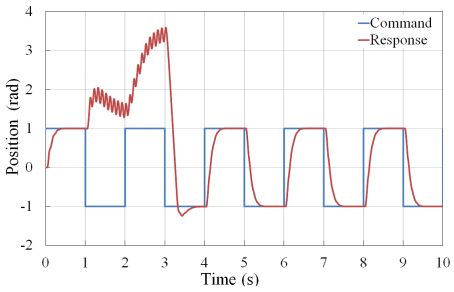

Figure 7: Experimental results of the conventional method without tamper detection

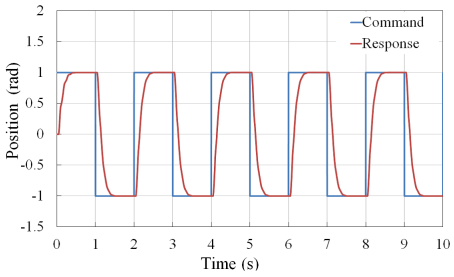

Figure 8: Experimental results of the proposed method with tamper detection

The conventional method which had only one forward path. Path 1 was affected by the tampering signal d_1. The position response could not track the position command while tampering signal was added . On the other hand, regardless of which path was tampered, the proposed method could select the correct control input. The position response could track the position command even if the tampering signals are injected on one of the forward paths. The experimental results showed that the proposed method could make the networked motion control system safe and secure by selecting correct control input appropriately.

5. Conclusion

This paper proposed the method using three redundant forward paths and the correct control input selection algorithm to achieve safe and secure operation of the networked motion control system. The experimental results showed that the proposed method could detect the tampered signal and select the correct control input appropriately. Our further studies include the consideration of transmission delay jitter and packet loss.

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] L. Zhang, H. Gao, and O. Kaynak, "Network-Induced Constraints in Networked Control Systems—A Survey," *IEEE Transactions on Industrial Informatics*, Vol. 9, No. 1, pp. 403–416, Feb. 2013.

[3] 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, Jul. 2010.

[4] J. Hespanha, P. Naghshtabrizi, and Y. Xu, "A Survey of Recent Results in Networked Control Systems," *Proceedings of the IEEE*, Vol. 95, No. 1, pp. 138–162, Jan. 2007.

[5] M. Nawir, A. Amir, N. Yaakob, and O. Lynn, "Internet of Things (IoT): Taxonomy of Security Attacks," *Proceedings of the 3rd International Conference on Electric Design, ICED*, pp. 321–326, Aug. 2016.

[6] S.M. Admin, and A.M. Giacomoni "Smart Grid—Safe, Secure, Self-Healing," *IEEE Power & Energy Magazine*, pp. 33–40, Jan./Feb. 2012.

[7] 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*, pp. 447–462, May 2010.

[8] A. Yassen and M. Bayart, "Attack-Tolerant Networked Control System Based on the Deception for the Cyber-Attacks," *Proceeding of the World Congress on Industrial Control Systems Security, WCICSS*, pp. 37–44, Dec. 2015.

[9] R. Muradore and D. Quaglia, "Energy-Efficient Intrusion Detection and Mitigation for Networked Control Systems Security," *IEEE Transactions on Industrial Informatics*, Vol. 11, No. 3, pp. 830–840, Jun. 2015.

[10] J. Hoshino, H. Kojima, T. Funakoshi, R. Imai, and R. Kubo, "Secure Networked Motion Control Using Tampering Detection Observer," *Proceedings of the 31st International Technical Conference on Circuits/Systems, Computers and Communications, ITC-CSCC*, pp. 613–616, Jul. 2016.

[11] 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*, D–T1–05, pp. 1–4, Jul. 2012.