ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 5, No. 3, 364-369 (2020)
www.astesj.com
Special Issue on Multidisciplinary Innovation in Engineering Science & Technology

ASTES Journal
ISSN: 2415-6698

Trajectory Tracking Control of a DC Motor Exposed to a Replay-Attack

Reda El Abbadi*, Hicham Jamouli

The Laboratory of System Engineering and Decision Law, National School of Applied Sciences Ibn Zohr University Agadir, Morocco.

ARTICLE INFO

Article history:
Received: 24 April, 2020
Accepted: 18 May, 2020
Online: 28 May, 2020

Keywords:
Networked control system
Replay-attack
Data packet dropout
Delay
Linear matrix inequalities

ABSTRACT

This paper investigates the trajectory tracking control (TTC) problem of a networked control system (NCS) against a replay-attack. The impact of data packet dropout and communication delay on the wireless network are taken into account. A new mathematical representation of the NCS under network issues (packet dropout, delay, and replay-attack) is proposed, the resulting closed-loop system is written in the form of an asynchronous dynamical system. Linear matrix inequalities (LMIs) formulation and a cone complementary linearization (CCL) approach are used to calculate the controller gain F_1 and the trajectory tracking gain F_2. Finally, a DC motor simulation with MATLAB is carried out to demonstrate the effectiveness of our approach.

1 Introduction

This article is an extended version of a conference paper presented in 2019 at the International Conference on Control and Fault-Tolerant Systems [1].

Networked Control System (NCS) is a new generation of systems where the control loop is closed through a communication network. The defining feature of an NCS is that system states and control law exchange between the components of the system (sensors, actuators, and controllers) in the form of information packages via a wireless network. The use of wireless network diminishes system wiring, simplifies maintenance and diagnosis, and improves the system agility [2, 3]. Nonetheless, the introduction of the wireless network to control the physical process brought some challenges, such as induced delay, and packet dropout, which harm the stability and reduce the system's performances. The model of the NCS with data packet dropout and network induced delay has been treated in [4–6]. There are also other challenges of using the network as a mean to impart the information between the system components, like malicious intrusions, viruses, and cyber-attackers who always find a way to access the system network and make critical damages. Consequently, reinforcing system security attracts the attention of the specialists. Remarkable papers have studied the security of the network and the cyber-attacks [7].

This article addresses a particular cyber-attack, termed as replay-attack, studied first in [8]. At our best knowledge, the trajectory tracking control (TTC) problem of NCS under a replay-attack based on an accurate mathematical model of the replay-attack is not fully investigated, and this will be the subject of this paper. In our previous work [1, 9, 10], we modeled the NCS under a replay-attack in three different ways. In [10], we used the Markovian jump linear system to model the replay-attack. In [1], we neglected the communication delay, and we assumed that the adversary attacks just the sensor reading, and in [9], we supposed that the adversary attacks the sensor reading and the actuator's inputs simultaneously. This article involves a new contribution compared to the studies mentioned above. In this study we will give a new model of the NCS against a replay-attack, in which we take into account the effect of the delay that exists in the communication channel (sensor-controller).

This extended version deals with the TTC of a DC motor controlled through a wireless network and exposed to a replay-attack. The adversary seeks to destabilize the system by recording secretly the sensor reading and subsequently replayed it to the controller. To protect its anonymity on the network and stay undetectable for the most prolonged period, the adversary appears at different times (randomly), that sounds similar to the Stuxnet cyber-attack [11]. Moreover, we will take into account the packet dropout and the delay in the communication channel (sensor-controller). Nevertheless, the communication channel (controller-actuator) will be supposed perfect, that means 100% of packets have successfully arrived at the actuator from the controller without any delay.

The study will contain four fundamental parts. We will start by

*Corresponding Author Email: reda.elabbadi@edu.uiz.ac.ma

defining the structure of the global system. Then, we will give the model of the network. After that, we will provide our model of the replay-attack. Finally, by using the linear matrix inequalities (LMIs) formulation and the cone complementary linearization (CCL) approach we will calculate the controller gain which helps us to find the TTC gain.

2 Structure of the Global System

The structure of the NCS against a replay-attack is given in Figure1. The sensor measurement $z(k_i)$, which has successfully arrived at the controller (the switch S1 is closed), will be first saved in a buffer. If a measurement $z(k_i)$ is lost during the transmission (the switch S1 is opened), the controller will utilize the measurements that are already stocked in the buffer to calculate the new control law $v(k_i)$. To avoid being detected by the classical detectors, the adversary will apply the attack at various times (randomly). The switch S2 models the replay-attack, if S2 is opened this means there is no attack in the buffer, whereas if S2 is closed this means there is an attack; this switching will harm the stability and the system's performances, which will reflect negatively on the trajectory tracking.

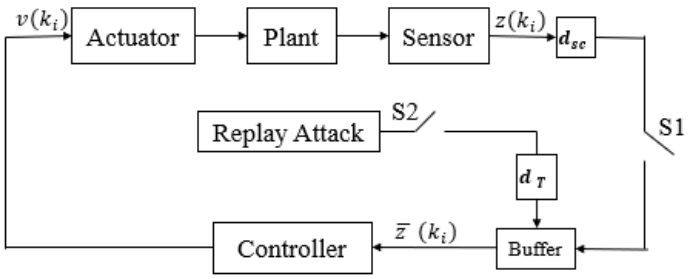

Figure 1: System architecture.

The plant of the system is defined as follows:

$$z(k_{i+1}) = Gz(k_i) + Hv(k_i), \tag{1}$$

where $z(k_i) \in \mathbb{R}^n$ is the system state and $v(k_i) \in \mathbb{R}^m$ is the control law. $G \in \mathbb{R}^{n\times n}$ is the state matrix and $H \in \mathbb{R}^{n\times m}$ is the input matrix. The state feedback controller is:

$$v(k_i) = F_1\bar{z}(k_i), \tag{2}$$

where F_1 is the controller gain, and $\bar{z}(k_i) \in \mathbb{R}^n$ is the controller input which will be defined in the next subsections.

2.1 Wireless network model

The iterative approach described in [12, 13] was adjusted to give a model of the wireless network with the packet dropout and the communication delay d_{sc} in the channel (sensor-controller).

The Figure 2 shows the packets sent from the sensor to the controller. The green packets represent the received packets, whereas the red ones represent the dropouts packets. The notations k_i and $k_i + m$ represent respectively the green packets and the red packets, where , $i \in \mathbb{Z}$ and , $m \in \mathbb{N}^*$.

At first, we will ignore the effect of the replay-attack and we will concentrate on the data packet dropout and the communication delay. Hence, the controller input can be written as:

$$\bar{z}(k_i) = z(k_{i-d_{sc}}). \tag{3}$$

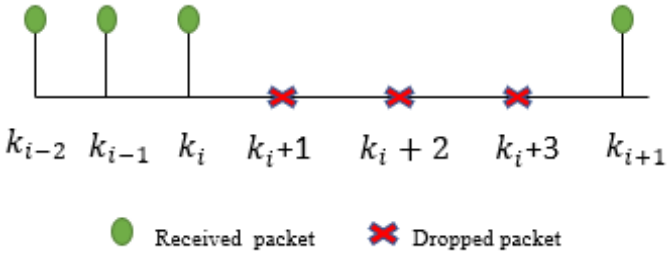

Figure 2: Received and lost packets [12].

As reported by Figure 2, the iterative approach can be defined as:

$$\begin{aligned}
z(k_i+1) &= Gz(k_i) + HF_1z(k_{i-d_{sc}}).\\
z(k_i+2) &= Gz(k_i+1) + HF_1z(k_{i-d_{sc}}),\\
&= G^2z(k_i) + GHF_1z(k_{i-d_{sc}}) + HF_1z(k_{i-d_{sc}}),\\
&= G^2z(k_i) + (GHF_1 + HF_1)z(k_{i-d_{sc}}).\\
z(k_i+3) &= Gz(k_i+2) + HF_1z(k_{i-d_{sc}}),\\
&= G^3z(k_i) + (G^2HF_1 + GHF_1 + HF_1)z(k_{i-d_{sc}}),
\end{aligned}$$

For time instant k_{i+1}, the mathematical model of the system with packet dropout and delay is:

$$z(k_{i+1}) = G^Nz(k_i) + \sum_{j=0}^{N-1} G^jHF_1z(k_{i-d_{sc}}), \tag{4}$$

with N is the number of successive dropped packets.

2.2 Replay-attack model

We assume that an attacker has connected to the buffer can replace the received packet $z(k_i)$ by the previous one $z(k_{i-d_T})$, with d_T is the replay-delay. For example, in the Figure 3 the third packet (102) was exposed to an attack with d_T=2T_e, so it was replaced by the first packet (100). The same for the packet (200) which was replaced by the packet (198).

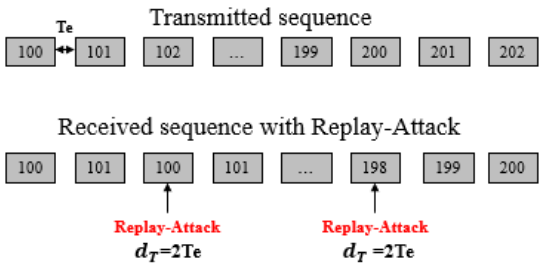

Figure 3: Replay-attack.

As reported by Figure 3, the system under a replay-delay can be defined as:

$$
\begin{aligned}
z(k_i+1) &= Gz(k_i) + HF_1 z(k_{i-d'_T}).\\
z(k_i+2) &= Gz(k_i+1) + HF_1 z(k_{i-d'_T}),\\
&= G^2 z(k_i) + GHF_1 z(k_{i-d'_T}) + HF_1 z(k_{i-d'_T}),\\
&= G^2 z(k_i) + (GHF_1 + HF_1) z(k_{i-d'_T}).\\
z(k_i+3) &= Gz(k_i+2) + HF_1 z(k_{i-d'_T}),\\
&= G^3 z(k_i) + (G^2HF_1 + GHF_1 + HF_1) z(k_{i-d'_T}).
\end{aligned}
$$

For time instant k_{i+1}, the mathematical model of the system against a replay-attack is:

$$z(k_{i+1}) = G^N z(k_i) + \sum_{j=0}^{N-1} G^j HF_1 z(k_{i-d'_T}), \tag{5}$$

where $d'_T = d_T + d_{sc}$.

The overall system will switch between two subsystems. Subsystem 1 if S2 is "off", and subsystem 2 if S2 is "on".
From (4) and (5) the global system becomes:

$$z(k_{i+1}) = G^N z(k_i) + \gamma \sum_{j=0}^{N-1} G^j HF_1 z(k_{i-d_{sc}}) + (1-\gamma) \sum_{j=0}^{N-1} G^j HF_1 z(k_{i-d'_T}), \tag{6}$$

where the variable γ equals one if S2 is "off", and equals zero if S2 is "on".
The augmented state can be written as:

$$\hat{z}(k_i) = [z^T(k_i)\, z^T(k_{i-1}) \cdots\ z^T(k_{i-d_{sc}}) \cdots\ z^T(k_{i-d'_T})]^T. \tag{7}$$

The overall system (6) can be written as:

$$\hat{z}(k_{i+1}) = \Phi_\sigma\, \hat{z}(k_i), \tag{8}$$

in which $\sigma = 1, 2$, and

$$\Phi_\sigma = \begin{bmatrix} G^N & 0 & \cdots & \gamma \sum_{j=0}^{N-1} G^j HF_1 \\ I & 0 & \cdots & 0 \\ 0 & I & 0 & \vdots \\ \vdots & \cdots & \ddots & \vdots \\ & & & \end{bmatrix} \begin{bmatrix} 0 & \cdots & (1-\gamma) \sum_{j=0}^{N-1} G^j HF_1 \\ \vdots & \cdots & 0 \\ \ddots & \ddots & \vdots \\ 0 & I & 0 \end{bmatrix}. \tag{9}$$

Therefore, the overall system can be equivalent to an asynchronous dynamical system expressed in (8),

with

$$\Phi_1 = \begin{bmatrix} G^N & 0 & \cdots & \sum_{j=0}^{N-1} G^j HF_1 \\ I & 0 & \cdots & 0 \\ 0 & I & 0 & \vdots \\ \vdots & \cdots & \ddots & \vdots \\ & & & \end{bmatrix} \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \cdots & 0 \\ \ddots & \ddots & \vdots \\ 0 & I & 0 \end{bmatrix}, \tag{10}$$

and

$$\Phi_2 = \begin{bmatrix} G^N & 0 & \cdots & 0 \\ I & 0 & \cdots & 0 \\ 0 & I & 0 & \vdots \\ \vdots & \cdots & \ddots & \vdots \\ & & & \end{bmatrix} \begin{bmatrix} 0 & \cdots & \sum_{j=0}^{N-1} G^j HF_1 \\ \vdots & \cdots & 0 \\ \ddots & \ddots & \vdots \\ 0 & I & 0 \end{bmatrix}. \tag{11}$$

3 Stability and Control Design

Lemma 1 *[14] The asynchronous dynamical system $z_{k+1} = f_s(z_k), s = 1...N'$, is exponential stable if there exists a Lyapunov function where $\beta_1\|z\|^2 \le V(z) \le \beta_2\|z\|^2$, $\beta_{1,2} > 0$, and given positive scalars α_s satisfying:*

$$V(z_{k+1}) - V(z_k) < (\alpha_s^{-2} - 1)V(z_k), \tag{12}$$

$$\alpha_1^{r_1}\alpha_2^{r_2}...\alpha_s^{r_s} > 0, \tag{13}$$

with r_s, ($s \in \mathbb{N}$) is the occur rate of discrete event satisfying this two conditions, $r_s > 0$ and $\sum_{s=1}^{N'} r_s = 1$.

Theorem 1 *If there exist symmetric matrices $P_1 > 0$, $P_2 > 0$ and given scalars $\alpha_\sigma > 0$, $\sigma = 1, 2$ satisfying:*

$$\alpha_1^r \alpha_2^{1-r} > 0, \tag{14}$$

$$\begin{bmatrix} -P_1 & \Phi_\sigma^T \\ \Phi_\sigma & -\alpha_\sigma^{-2} P_2 \end{bmatrix} < 0, \tag{15}$$

with minimizing the trace ($P_1.P_2$) subject to:

$$\begin{bmatrix} P_1 & I \\ I & P_2 \end{bmatrix} \geqslant 0. \tag{16}$$

Then, the system (8) is exponential stable.

Proof: applying (12) to (8), we have

$$V(\hat{z}_{k_{i+1}}) - V(\hat{z}_{k_i}) < (\alpha_\sigma^{-2} - 1)V(\hat{z}_{k_i}).$$

Hence,

$$V(\hat{z}_{k_{i+1}}) < \alpha_\sigma^{-2} V(\hat{z}_{k_i}).$$

Since $V(\hat{z}_{k_i}) = \hat{z}^T(k_i)P_1^{-1}\hat{z}(k_i)$,

$$\hat{z}^T(k_i)\Phi_\sigma^T P_1^{-1}\Phi_\sigma\hat{z}(k_i) < \alpha_\sigma^{-2}\hat{z}^T(k_i)P_1^{-1}\hat{z}(k_i).$$

Therefore,

$$\Phi_\sigma^T P_1^{-1}\Phi_\sigma - \alpha_\sigma^{-2}P_1^{-1} < 0. \tag{17}$$

To rewrite (17) in a matrix form. We will utilize the Schur compliment. Then, (17) becomes:

$$\begin{bmatrix} -P_1 & \Phi_\sigma^T \\ \Phi_\sigma & -\alpha_\sigma^{-2}P_1^{-1} \end{bmatrix} < 0. \tag{18}$$

Remark 1 *It is clear that* (18) *is not linear because of the existence of* P_1 *and its inverse* P_1^{-1} *in the same matrix. To fix this problem we will make a change of variable* ($P_2 = P_1^{-1}$)*, and to guarantee the convergence of* P_2 *to* P_1^{-1}*, we will use the CCL approach [15]. The inequality matrices* (18) *becomes:*

$$\begin{bmatrix} -P_1 & \Phi_\sigma^T \\ \Phi_\sigma & -\alpha_\sigma^{-2}P_2 \end{bmatrix} < 0, \tag{19}$$

with

$$P_2 = P_1^{-1}. \tag{20}$$

The CCL approach is an algorithm used to guarantee that, P_2 equals P_1^{-1}, by minimizing the trace ($P_1.P_2$) subject to:

$$\begin{bmatrix} P_1 & I \\ I & P_2 \end{bmatrix} \geqslant 0. \tag{21}$$

Solving the LMIs using Yalmip Toolbox, we can calculate the gain F_1 which will help us to find the trajectory tracking gain F_2.

$$F_2^{-1} = C(I - (G + HF_1))^{-1}H. \tag{22}$$

4 Application

4.1 DC motor Model

A DC motor is a machine which converts direct current electrical power into mechanical power. The DC motor has vast applications in many fields including NCS. Owing to this importance, we chose the DC motor as an application system where we will apply our approach.

In this paragraph, the mathematical model of a DC motor will be studied.

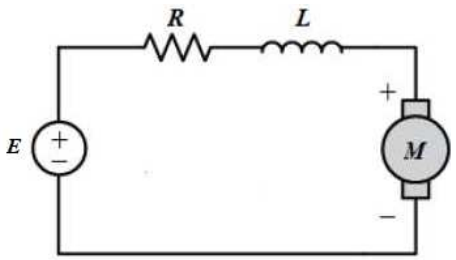

Figure 4: DC motor equivalent circuit model.

As shown in Figure 4, the system input is the voltage source (E), while the system output is the rotational speed $\dot{\theta}$. The physical parameters of the DC motor are given in Table 1:

Table 1: Physical parameters of the Dc motor.

Symbol	Description	Value
J	Moment of inertia	0.02 Kg.m^2
b	Motor viscous friction constant	0.2 N.m.s
K_e	Constant of emf	0.02V.s/rad
K_t	Motor torque constant	0.02N.m/A
R	Resistance	1.5 Ω
L	Inductance	0.5H

The motor torque and the back emf (e) are given in (23) and (24):

$$T_q = K_t.i, \tag{23}$$

$$e = K_e.\dot{\theta}. \tag{24}$$

Let us consider the constant K such that $K = K_t = K_e$. From the Figure 4, and employing the Kirchhoff's voltage law, the electrical equation of the DC motor is described as:

$$J\ddot{\theta} + b\dot{\theta} = Ki, \tag{25}$$

$$L\frac{di}{dt} + Ri = E - K\dot{\theta}. \tag{26}$$

If we choose $[\dot{\theta}, i]^T$ as a state variables, the state space representation will be written as:

$$A = \begin{bmatrix} \frac{-b}{J} & \frac{K}{J} \\ \frac{-K}{L} & \frac{-R}{L} \end{bmatrix}, B = \begin{bmatrix} 0 \\ \frac{1}{L} \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \end{bmatrix}, \text{D} = 0.$$

Replacing the parameters by their values, the state space representation becomes:

$$A = \begin{bmatrix} -10 & 1 \\ -0.04 & -3 \end{bmatrix}, B = \begin{bmatrix} 0 \\ 2 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \end{bmatrix}, \text{D} = 0.$$

The command "c2d" in Matlab is used to passe from the continuous-time to discrete-time, where the sampling time is $T_e = 0.1s$. The discrete-system can be written as follow:

$$G = \begin{bmatrix} 0.3678 & 0.0563 \\ -0.0021 & 0.7407 \end{bmatrix}, H = \begin{bmatrix} 0.0066 \\ 0.1728 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \end{bmatrix}, \text{D} = 0.$$

4.2 Simulation and results

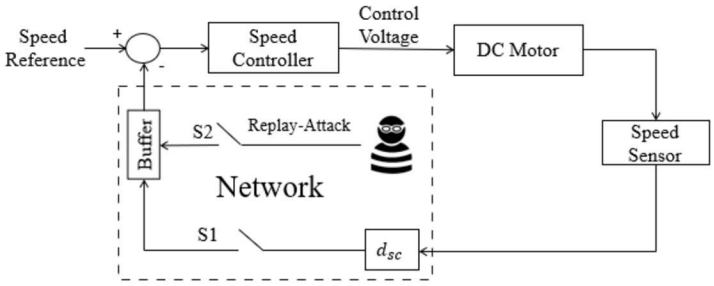

Figure 5: DC motor control under network issues.

The Figure 5 shown the structure of the DC motor under wireless network issues. The initial condition is $z(0) = [0 \;\; 0]^T$, $v_i = 0$, for $i \leq 0$, the maximum number of the successive packets losses during the transmission is N=3 packets, the communication delay equals to 0.1s, and the replay-delay equals to 0.3s, that means $d_{sc} = 1$, and d_T=3. We will study three different situations. In the first situation, the event rate of the switch S2 equals 0.1, in the second situation, the event rate equals 0.5, in the third, the event rate equals 0.9.

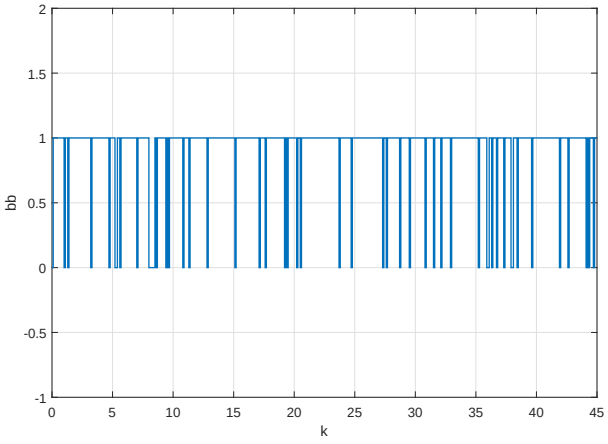

Figure 6: Event rate of S2 is 0.1.

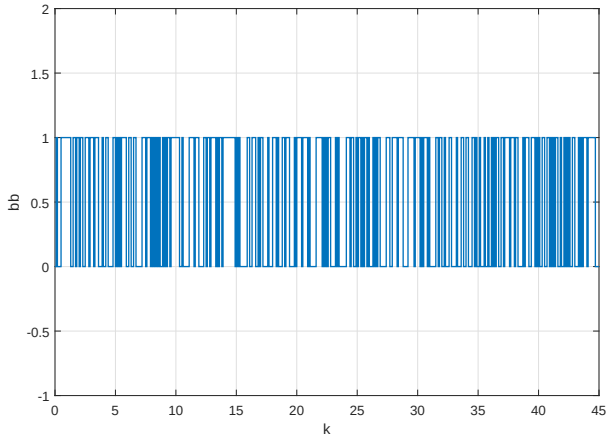

Figure 7: Event rate of S2 is 0.5.

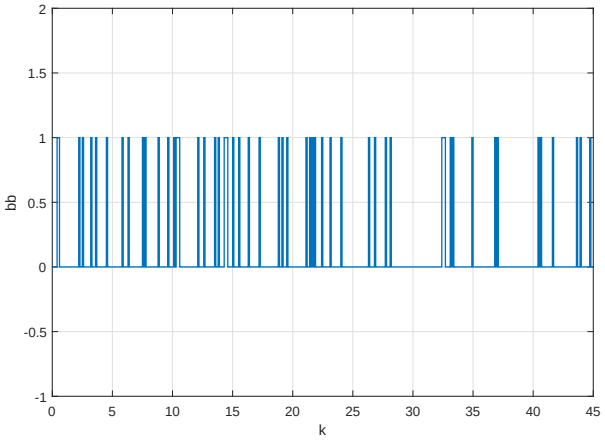

Figure 8: Event rate of S2 is 0.9.

The figures (Figure 6, Figure 7, Figure 8) show the different event rate of the switch S2. 0.1, 0.5 and 0.9 respectively.

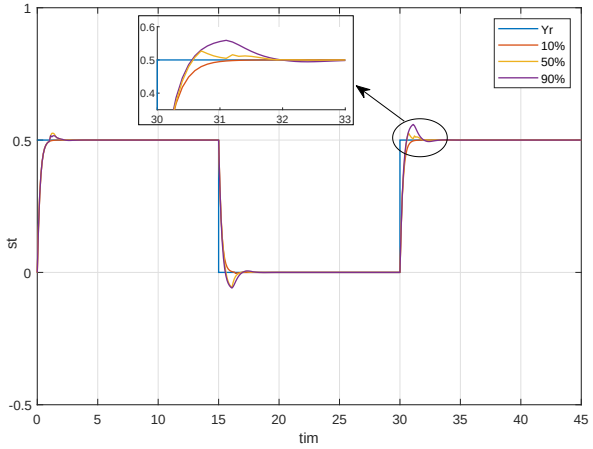

Figure 9: Trajectory tracking.

According to Theorem 1, the LMIs are feasible for $\alpha_1 = 0.1$ and $\alpha_2 = 0.45$. Solving the LMIs in Theorem 1 utilizing the Yalmip toolbox, we can find the controller gain and the trajectory tracking gain of the system as follow:
$F_1 = [0 \;\; 0.0012]$ and $F_2 = 20.9085$.

From Figure 9, we can see that if the event rate of the switch S2 equals 0.1 (the percentage to have an attack is 10%) the output can tracks perfectly the trajectory Y_r, the same thing happens if the chance to have an attack rises to 50% or 90%. But, in these two cases an overshoot appears. However, the results stay acceptable, which reflects the potency of our approach.

5 Conclusion

This paper dealt with the TTC issue of a DC motor controlled through a wireless network. In this extended version, we took into account the packet dropout and the delay in the communication channel (sensor-controller). On the other hand, the communication channel (controller-actuator) was assumed perfect, that means all

data have successfully transferred from the controller to the actuator without any delay. We also considered that the DC motor exposed to a replay-attack, where a cyber-adversary sought to destabilize the system and diminished its performances. A new mathematical model of the NCS under replay-attack was proposed. A sufficient condition for the stability of the resulting asynchronous dynamical system was given in the form of LMIs. The controller gain F_1 and the trajectory tracking gain F_2 were obtained by solving these LMIs employing the CCL approach. Finally, the simulation results proved the effectiveness of our approach. As a perspective of this study, our attention will be oriented towards studying the same problem with communication delay and packets losses in both communication channels.

References

[1] R. El Abbadi and H. Jamouli, "Stabilization of cyber physical system with data packet dropout and replay attack via switching system approach," in *2019 4th Conference on Control and Fault Tolerant Systems (SysTol)*. IEEE, 2019, pp. 325–329, doi: 10.1109/SYSTOL.2019.8864787.

[2] T. C. Yang, "Networked control system: a brief survey," *IEE Proceedings-Control Theory and Applications*, vol. 153, no. 4, pp. 403–412, 2006, doi: 10.1049/ip-cta:20050178.

[3] J. P. 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, 2007, doi: 10.1109/JPROC.2006.887288.

[4] J. Xiong and J. Lam, "Stabilization of linear systems over networks with bounded packet loss," *Automatica*, vol. 43, no. 1, pp. 80–87, 2007, doi: 10.1016/j.automatica.2006.07.017.

[5] L. Qiu, Q. Luo, S. Li, and B. Xu, "Modeling and output feedback control of networked control systems with both time delays; and packet dropouts," *Mathematical Problems in Engineering*, vol. 2013, 2013, doi: 10.1155/2013/609236.

[6] L. Qiu, Q. Luo, F. Gong, S. Li, and B. Xu, "Stability and stabilization of networked control systems with random time delays and packet dropouts," *Journal of the Franklin Institute*, vol. 350, no. 7, pp. 1886–1907, 2013, doi: 10.1016/j.jfranklin.2013.05.013.

[7] J. M. R. Hernan, "Detection of attacks against cyber-physical industrial systems," Ph.D. dissertation, 2017.

[8] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, 2009, pp. 911–918, doi: 10.1109/ALLERTON.2009.5394956.

[9] R. EL Abbadi and H. Jamouli, "Stabilization of a cyber physical system with network issues," in *2019 8th International Conference on Systems and Control (ICSC)*. IEEE, 2019, pp. 508–512, doi: 10.1109/ICSC47195.2019.8950544.

[10] R. El Abbadi and H. Jamouli, "Stabilization of cyber physical system exposed to a random replay attack modeled by markov chains," in *2019 6th International Conference on Control, Decision and Information Technologies (CoDIT)*. IEEE, 2019, pp. 528–533, doi: 10.1109/CoDIT.2019.8820311.

[11] P. Shakarian, J. Shakarian, and A. Ruef, "Attacking iranian nuclear facilities: Stuxnet," *Introduction to cyber-warfare: A multidisciplinary approach*, pp. 223–239, 2013, doi: 10.1016/B978-0-12-407814-7.00013-0.

[12] A. Routh, S. Das, and I. Pan, "Stabilization based networked predictive controller design for switched plants," in *2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12)*. IEEE, 2012, pp. 1–6, doi: 10.1109/ICCCNT.2012.6396001.

[13] M. Yu, L. Wang, T. Chu, and G. Xie, "Stabilization of networked control systems with data packet dropout and network delays via switching system approach," in *2004 43rd IEEE Conference on Decision and Control (CDC)(IEEE Cat. No. 04CH37601)*, vol. 4. IEEE, 2004, pp. 3539–3544, doi: 10.1109/CDC.2004.1429261.

[14] A. Rabello and A. Bhaya, "Stability of asynchronous dynamical systems with rate constraints and applications," *IEE Proceedings-Control Theory and Applications*, vol. 150, no. 5, p. 546, 2003, doi: 10.1049/ip-cta:20030704.

[15] L. El Ghaoui, F. Oustry, and M. AitRami, "A cone complementarity linearization algorithm for static output-feedback and related problems," *IEEE transactions on automatic control*, vol. 42, no. 8, pp. 1171–1176, 1997, doi: 10.1109/9.618250.