Fuzzy Weighted Memory Event-Triggered Control for Networked Control Systems Subject to Deception Attacks

Mohamed Rouamel, Fayçal Bourahala, Kevin Guelton, Samir Bouzoualegh, Laurent Arcese

Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnLine 55-15 (2022) 45–50

Fuzzy Weighted Memory Event-Triggered Control for Networked Control Systems Subject to Deception Attacks

Mohamed Rouamel * **Fayçal Bourahala** * **Kevin Guelton** **
Samir Bouzoualegh * **Laurent Arcese** **

* *Department of Electrical Engineering, LAS Laboratory, 20 August University, 21000 Skikda, Algeria, (e-mail: {m.rouamel,f.bourahala}@univ-skikda.dz)*
** *CReSTIC EA3804 - Université de Reims Champagne-Ardenne, Moulin de la Housse BP1039, 51100 Reims, France, (e-mail: {kevin.guelton,laurent.arcese}@univ-reims.fr)*

Abstract: This paper considers the event-triggered control problem for a class of Networked Control Systems (NCS) subject to transmission delays and stochastic deception attacks. A new fuzzy weighted memory event-triggered mechanism is proposed to reduce the network bandwidth consumption and data transmission rates. In this context, a new fuzzy weighted memory state feedback controller is proposed to stabilize the closed-loop NCS. Considering the security problem of NCS, a randomly occurring deception attack model is employed, assuming bounded malicious signals injected by the attacker. Based on a suitable Lyapunov-Krasovskii functional, a design methodology is proposed, in terms of linear matrix inequalities, to synthesize both trigger parameters and NCS controller gains. Finally, a numerical example is considered to illustrated the effectiveness of proposed results, compared to previous ones from the literature.

Keywords: Networked control systems, Event-triggered Controller design, Deception Attacks.

1. INTRODUCTION

In the real world, control systems are often implemented via digital platforms, where the control components (sensors, controllers, actuators) are connected through a digital communication channel. Such control topology, known as Networked Control System (NCS), recently become an important research field. Indeed, NCSs allow to reduce implementation costs with easy installation and high reliability (Qiu et al., 2013; Rouamel et al., 2020). In NCSs, sampled-data control approaches are adopted in many works, e.g. (Lopes et al., 2021; Nafir et al., 2021; Rouamel et al., 2022). The sampling period under this scenario is often set as small as possible to guarantee desired closed-loop dynamics, despite a great number of redundant released packets. However, the transmission of a large amount of data may lead to unanticipated disadvantages, such as network congestion, data collisions, buffer overflow, and so may impose a huge burden on the communication channel (Tian et al., 2019). To cope with the reduction of released data in NCSs, Event-Triggered Schemes (ETSs) are considered in many recent works, e.g. (Tian et al., 2019; Rouamel et al., 2021). Usually, the triggering conditions are based on the difference between the current sampled signal and its last release. Hence, to avoid releasing packets when such a difference is small, memory event-triggered schemes (METS) have been recently proposed by considering historic released signals (memory) in the ETS conditions, providing a good trade-off between the performances of the closed-loop system and the network load (Wang et al., 2020; Sun et al., 2021; Rouamel et al., 2021).

Moreover, it is worth noticing that NCSs can be corrupted by cyber-attacks, leading to loss of stability guarantees and so security breaches and impairments (Zhang and Guo, 2021). Three types of cyber-attacks are often considered in the literature: Denial of Service (DoS) attacks, replay attacks and deception attacks (Ding et al., 2017; Cao et al., 2021). DoS attacks can block the communication channel. Replay attacks usually replace the current transmitted signals by past ones. Deception attacks replace the originally transmitted signals by malicious ones, providing harmful consequences to the NCS security. Several recent works have been done to cope with such issue, especially by considering that the NCS is subject to stochastic deception attacks, e.g. (Wang et al., 2020; Sun et al., 2021). The design of NCS subject to deception attacks remains on the stability analysis of closed-loop systems with input time-varying delays, disturbed by stochastic entries. The stability analysis is often made via Lyapunov-Krasovskii Functionals (LKF) in the Linear Matrix Inequality (LMI) framework, but with conservatism. Hence, relaxing the conservatism may help to improve the resilience against deception attacks of the designed closed-loop NCS, which is the goal followed in the present study.

The main contribution of this paper is to propose a new Fuzzy Weighted Memory Event-Triggered Mechanism (FWMETM) to mitigate the network loads in NCSs, with the design of a new stabilizing fuzzy weighted memory state feedback networked controller, such that the robustness against deception attacks is improved for the designed closed-loop NCSs. The main idea being to schedule the ac-

10.1016/j.ifacol.2022.07.606

tual and memory data according to a fuzzy blending mechanism, which makes preponderant the actual data during fast transients, while memory data is mostly considered when the NCS gets closer to its equilibrium. Moreover, to cope with the security problem of NCSs, randomly occurring deception attacks are considered, i.e. where bounded malicious signals are injected by the attacker. Based on the proposed FWMETM, new relaxed LMIs-based design conditions for both the trigger parameters and the NCS controller gains will be proposed from the choice of a suitable convenient LKF. Then, the proposed NCS design methodology will be illustrated and compared to previous related results through a numerical example in simulation.

*Notations. In the sequel, stars * in matrices denote bloc transpose quantities. For a square matrix M, one denotes $\mathcal{H}(M)=M+M^T$. $M>0$ (<0) denotes a positive (negative) definite matrix M. $\|.\|_2$ stands for the $L_2[0,\infty)$ norm. For column vectors $v_1, \ldots, v_n$, $\mathrm{col}\{v_1, v_2, ..., v_n\} = [v_1^T \ldots v_n^T]^T$. A finite set of r positive integers is denoted $\mathcal{I}_r = \{1, ..., r\}$. Also, $\forall j \in \mathcal{I}_{12}$, we denote the block entry matrices $e_j = \left[\, 0_{n\times(j-1)n} \;\; I_{n\times n} \;\; 0_{n\times(12n-j)n} \,\right]^T \in R^{12n\times n}$, for example: $e_4 = [0\;0\;0\;I\;0\;0\;\ldots\;0\;0]^T$. Finally, for any square matrix X and identity matrix I with the same dimension, we denote the diagonal bloc matrix $D_X = \mathrm{diag}\{\underbrace{X \ldots X}_{10\ times}\; I\; I\}$.*

2. PRELIMINARIES

The block diagram of the considered NCS under the proposed Event-Triggered mechanism and subject to network-induced delay and deception attack is shown in Fig. 1.

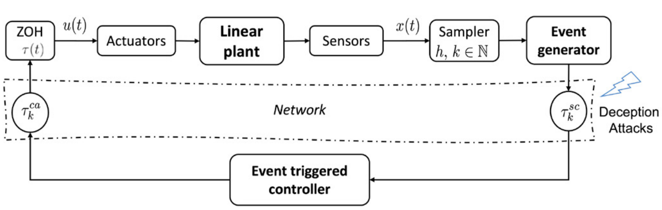

Fig. 1. NCS under ETS and deception attacks.

In this NCS scheme, we assume that the plant to be controlled is represented by the linear state space equation:

$$\dot{x}(t) = Ax(t) + Bu(t) \tag{1}$$

where $x(t) \in \mathbb{R}^n$ and $u(t) \in \mathbb{R}^\nu$ are the state and input vectors, $A \in \mathbb{R}^{n\times n}$ and $B \in \mathbb{R}^{n\times\nu}$ are constant matrices.

We are concerned with the closed-loop stabilization of (1) through a network from event-triggered sampled-data state feedback under the following assumptions.

Assumption 1. The state variables are available from measurements. Their values are broadcast together as single-packets at each sampling instant to the controller device.

Assumption 2. We assume that the sensors are clock-driven with a fixed sampling period h and the controller and actuators are event driven from the FWMETM.

Let $k \in \mathbb{N}$ be the actual sampling number, we denote τ_k^{sc} and τ_k^{ca}, respectively the sensors to controller and the controller to actuators network-induced delays, and so $\tau_k = \tau_k^{sc} + \tau_k^{ca}$ the overall network-induced delay. To mitigate the transmissions of data through the network and so saving the its bandwidth, we propose, for the event generator, a new FWMETM. That is to say, to decide whether the current sampling state measurements should be transmitted or not to the controller over the network, the next transmission instant t_{k+1} satisfies:

$$t_{k+1} = t_k + \min_{l\in\mathbb{N}^\star}\left\{ lh \,\middle|\, \sum_{i=1}^{2} \varsigma_i(x(t_k)) e^T(t_{k-i+1}) \Omega_i e(t_{k-i+1}) > \rho \sum_{i=1}^{2} \varsigma_i(x(t_k)) x^T(t_{k-i+1}) \Omega_i x(t_{k-i+1}) \right\} \tag{2}$$

where, $\forall i \in \mathcal{I}_2$, $e(t_{k-i+1}) = x(t_{k-i+1}) - x(t_k + lh)$ denotes respectively the errors between the current $(i=1)$ or the previous $(i = 2)$ released packets and the most recent sampled instant, $\rho \in [0, 1]$ is a pre-fixed event triggered threshold, $\Omega_i > 0$ are event triggering weighting matrices to be designed, and $\varsigma_i(x(t_k))$ are fuzzy weighting functions for the actual $(i=1)$ and memory $(i=2)$ data given as:

$$\varsigma_1(x(t_k)) = \mu\left(1 - e^{-\lambda\|x(t_k)\|_2}\right),\; \varsigma_2(x(t_k)) = 1 - \varsigma_1(x(t_k)) \tag{3}$$

with $\mu \in [0, 1]$ and $\lambda > 0$ pre-fixed, so that $\varsigma_1(x(t_k)) \in [0, \mu]$, $\varsigma_2(x(t_k)) \in [1-\mu, 1]$ and $\varsigma_1(x(t_k)) + \varsigma_2(x(t_k)) = 1$.

Remark 1. With the FWMETM condition (2) and the dynamics weighting functions (3), it is to be highlighted that the parameters ρ, μ and λ can be tuned according to the user needs. For instance, ρ can be used to mitigate the number of realised event-triggered packets when it is chosen as big as possible, see e.g. (Tian et al., 2019). Moreover, when μ is chosen closed to 1, this means that the actual data is mostly selected from the FWMETM during the transients (i.e. $||x(t_k)||_2 >> 0$), while memory data are mostly selected when the system get closer to its equilibrium point (i.e. $||x(t_k)||_2 \to 0$). Finally, the choice of the decay rate λ allows to set how fast the changes occur in the FWMETM to weight the actual and memory data.

With the considered NCS, the ZOH allows to keep the control signal constant during the interval $\mathbb{I}_z = [t_k + \tau_k, t_{k+1} + \tau_{k+1})$, which can be divided, similarly the way borrowed in (Yue et al., 2012), into several sub-intervals such that $\mathbb{I}_z = \bigcup_{l=0}^{\bar{v}} \mathbb{I}_l$ with:

$$\mathbb{I}_z = \begin{cases} \mathbb{I}_{l=0} = [t_k + \tau_k, t_k + h + \tau_k),\; l = 0 \\ \mathbb{I}_l = [t_k + lh + \bar{\tau}, t_k + lh + h + \bar{\tau}),\; l = 1, 2, \ldots, \bar{v} - 1 \\ \mathbb{I}_{l=\bar{v}} = [t_k + \bar{v}h + \bar{\tau}, t_{k+1} + \tau_{k+1}),\; l = \bar{v} \end{cases}$$

where $\bar{\tau} = \max_{k\in N} \tau_k$ and $\bar{v} \in \mathbb{N}$ satisfies $t_k + \bar{v}h + \bar{\tau} < t_{k+1} + \tau_{k+1} \leq t_k + \bar{v}h + h + \bar{\tau}$. Moreover, $\forall t \in \mathbb{I}_z$, let $\tau(t) = t - t_k - lh$, which satisfies $0 \leq \tau_1 \leq \tau_k \leq \tau(t) \leq \bar{\tau} + h = \tau_2$ and $\dot{\tau}(t) = 1$. Hence we can write $x(t_k + lh) = x(t - \tau(t))$ and, in this FWMETM context, we propose the following sampled-data control law with fuzzy weighted memory action:

$$\begin{aligned} u(t) &= \sum_{i=1}^{2} \varsigma_i(x(t_k)) K_i x(t_{k-i+1}) \\ &= \sum_{i=1}^{2} \varsigma_i(x(t_k)) K_i (x(t - \tau(t)) + e(t_{k-i+1})) \end{aligned} \tag{4}$$

where $K_1, K_2 \in \mathbb{R}^{\nu\times n}$ are gain matrices to be synthesized.

Moreover, in this paper, we assume that the communication network is vulnerable to an attacker who can alter the transmitted information. In this context, we assume that the system's state $x(t_k)$ can be captured by the attacker, which replace it by an aggressive signal $f(x(t_k))$, released in a random way. When such deception attacks occur, the faked signal would join in the buffer of the controller together with the true signal. It is hard to distinguish the faked signals from the non attacked one. To get rid of this dilemma, similarly to what is proposed in (Wang et al., 2020), the following assumption is made.

Assumption 3. At every released instants, the event generator will packet a historic released signal $\{x(t_k), x(t_{k-1})\}$ and send them together to the controller.

In this case, under randomly occurring deception attacks, the control law (4) is modified as:

$$
\begin{aligned}
u(t) = &(1-\sigma(t))\sum_{i=1}^{2} \varsigma_i(x(t_k))K_i(x(t-\tau(t))+e_{k-i+1}(t)) \\
&+ \sigma(t)\sum_{i=1}^{2} \varsigma_i(f(x(t_k)))K_i f_i(x(t_k))
\end{aligned} \tag{5}
$$

where $\sigma(t) \in \{0,1\}$ is the occurring function of the deception attacks. That is to say, there are no attacks when $\sigma(t) = 0$ and, when $\sigma(t) = 1$, the original signals $\{x(t_k), x(t_{k-1})\}$ are replaced by the attacker as a set of aggressive signals $\{f(x(t_k)), f(x(t_{k-1}))\}$.

Therefore, similarly to what is done in related works, see e.g. (Wang et al., 2020), the following assumption is made.

Assumption 4. The mathematical expectation $\bar{\sigma}$ of $\sigma(t)$ is assumed to be known (i.e. $\mathbb{E}(\sigma(t)) = \bar{\sigma}$), and $f(x(t_k))$ is assumed to satisfy:

$$||f(x(t_k))||_2 \leq ||Gx(t_k)||_2 \tag{6}$$

where G is a known matrix representing the upper bound of the nonlinearity $f(.)$.

Substituting (5) into (1), yields the expression of the closed-loop dynamics:

$$
\begin{aligned}
\dot{x}(t) = \sum_{i=1}^{2}\sum_{j=1}^{2} &\varsigma_i(x(t_k))\varsigma_j(f(x(t_k)))\Big(Ax(t) \\
&+\sigma(t)BK_j f(x(t-\tau(t)) \\
&+(1-\sigma(t))BK_i(x(t-\tau(t))+e(t_{k-j+1}))\Big)
\end{aligned} \tag{7}
$$

Problem statement. The goal of this work is to provide LMI-based conditions for the design of the gains matrices K_1 and K_2 of the fuzzy weighting event-triggered controller (5), minimizing the number of redundant released packets, such that the closed-loop dynamics (7) is globally asymptotically stable and resilient to bounded deception attacks (see assumption 4).

3. MAIN RESULT

The following theorem summarizes the proposed LMI-based conditions, satisfying the above problem statement.

Theorem 1. For given scalars $\tau_2 \geq \tau_1 > 0$, $\rho > 0$, $\epsilon_1 > 0$, $\epsilon_2 > 0$, δ, μ and $\bar{\sigma}$, the closed-loop NCS (7) is globally asymptotically stabilized by the networked controller (5), subject to deception attack under assumption 4, under the release instants defined by the FWMETM condition (2), if there exist the real matrices, $X > 0$, $\tilde{P} > 0$, $\tilde{Q}_1 > 0$, $\tilde{Q}_2 > 0$, $\tilde{Q}_3 > 0$, $\tilde{R}_1 > 0$, $\tilde{R}_2 > 0$, $\tilde{\Omega}_1$, $\tilde{\Omega}_2$, $\tilde{\mathcal{W}}$, $\tilde{S}_{11}$, $\tilde{S}_{12}$, $\tilde{S}_{13}$, $\tilde{S}_{22}$, $\tilde{S}_{23}$, $\tilde{S}_{33}$, $\tilde{L}$, $\tilde{K}_1$ and $\tilde{K}_2$ with appropriate dimensions such that the following LMIs hold, $\forall q \in \mathcal{I}_2$ and $\forall \ell \in \mathcal{I}_4$:

$$\begin{bmatrix} \tilde{\mathcal{R}}_2 & \tilde{\mathcal{W}} \\ \tilde{\mathcal{W}}^T & \tilde{\mathcal{R}}_2 \end{bmatrix} > 0, \tag{8}$$

$$\tilde{\Phi} + \tilde{\Xi}_q + \tilde{\Psi}_\ell + \mathcal{H}\left(e_1^T \tilde{P} e_8 + \mathcal{E} Z_\ell\right) < 0, \tag{9}$$

where $\mathcal{E} = \left[\, I \ 0 \ \epsilon_1 I \ 0 \ 0 \ 0 \ 0 \ \epsilon_2 I \ 0 \ 0 \ 0 \ 0 \,\right]^T$,

$$
\begin{aligned}
Z_1 =&\big[AX \ 0 \ (1-\bar{\sigma})(1-\mu)B\tilde{K}_2 \ 0 \ 0 \ 0 \ 0 -X \\
&\ldots 0 \ (1-\mu)(1-\bar{\sigma})B\tilde{K}_2 \ 0 \ (1-\mu)\bar{\sigma}B\tilde{K}_2\big], \\
Z_2 =&\big[AX \ 0 \ (1-\bar{\sigma})(1-\mu)B\tilde{K}_2 \ 0 \ 0 \ 0 \ 0 -X \\
&\ldots 0 \ (1-\mu)(1-\bar{\sigma})B\tilde{K}_2 \ \mu\bar{\sigma}B\tilde{K}_1 \ \bar{\sigma}B\tilde{K}_2\big], \\
Z_3 =&\big[AX \ 0 \ (1-\bar{\sigma})B(\mu\tilde{K}_1+\tilde{K}_2) \ 0 \ 0 \ 0 \ 0 -X \\
&\ldots \mu(1-\bar{\sigma})B\tilde{K}_1 \ (1-\bar{\sigma})B\tilde{K}_2 \ 0 \ (1-\mu)\bar{\sigma}B\tilde{K}_2\big], \\
Z_4 =&\Big[AX \ 0 \ (1-\bar{\sigma})B(\mu\tilde{K}_1+\tilde{K}_2) \ 0 \ 0 \ 0 \ 0 -X \\
&\ldots \mu(1-\bar{\sigma})B\tilde{K}_1 \ (1-\mu)(1-\bar{\sigma})B\tilde{K}_2 \ \mu\bar{\sigma}B\tilde{K}_1 \ \bar{\sigma}B\tilde{K}_2\big], \\
\tilde{\Phi} =& e_1^T\tilde{Q}_1e_1 - e_2^T\tilde{Q}_1e_2 - e_4^T\tilde{Q}_2e_4 + \chi_0^T\tilde{\mathcal{R}}_1\chi_0 \\
&+ e_8^T(\tau_1^2\tilde{R}_1+(\tau_2-\tau_1)^2\tilde{R}_2)e_8 - \begin{bmatrix}\chi_1\\ \chi_2\end{bmatrix}^T \begin{bmatrix}\tilde{\mathcal{R}}_2 & \tilde{\mathcal{W}}\\ * & \tilde{\mathcal{R}}_2\end{bmatrix}\begin{bmatrix}\chi_1\\ \chi_2\end{bmatrix}, \\
\tilde{\Xi}_1 =& -\underline{\chi}_3^T\begin{bmatrix}\tilde{S}_{11} & \tilde{S}_{12} & \tilde{S}_{13}\\ * & \tilde{S}_{22} & \tilde{S}_{23}\\ * & * & \tilde{S}_{33}\end{bmatrix}\underline{\chi}_3 + \frac{1}{\tau_1}\begin{bmatrix}e_1\\ e_3\end{bmatrix}^T\begin{bmatrix}-\tilde{L} & \tilde{L}\\ * & -\tilde{L}\end{bmatrix}\begin{bmatrix}e_1\\ e_3\end{bmatrix} \\
&+ (\tau_2-\tau_1)\left(\mathcal{H}\Big(\underline{\chi}_3^T\begin{bmatrix}\tilde{S}_{11} & \tilde{S}_{12} & \tilde{S}_{13}\\ * & \tilde{S}_{22} & \tilde{S}_{23}\\ * & * & \tilde{S}_{33}\end{bmatrix}\chi_4\Big) + e_8^T\tilde{L}e_8\right), \\
\tilde{\Xi}_2 =& -\bar{\chi}_3^T\begin{bmatrix}\tilde{S}_{11} & \tilde{S}_{12} & \tilde{S}_{13}\\ * & \tilde{S}_{22} & \tilde{S}_{23}\\ * & * & \tilde{S}_{33}\end{bmatrix}\bar{\chi}_3 + \frac{1}{\tau_2}\begin{bmatrix}e_1\\ e_3\end{bmatrix}^T\begin{bmatrix}-\tilde{L} & \tilde{L}\\ * & -\tilde{L}\end{bmatrix}\begin{bmatrix}e_1\\ e_3\end{bmatrix}, \\
\tilde{\Psi}_1 =& \tilde{\Psi}_3 = (1-\mu)\rho e_3^T\tilde{\Omega}_2e_3 + (1-\mu)\rho e_3^T\tilde{\Omega}_2e_{10} \\
&+2\bar{\sigma}e_3^TG^TGe_3 + \bar{\sigma}\mathcal{H}(e_3^TG^TGe_9) + \bar{\sigma}\mathcal{H}(e_3^TG^TGe_{10}) \\
&-\bar{\sigma}e_9^TG^TGe_9 + \bar{\sigma}e_{10}^TG^TGe_{10} - \bar{\sigma}e_{11}^Te_{11} - \bar{\sigma}e_{12}^Te_{12} \\
&+(\rho-1)(1-\mu)e_{10}^T\tilde{\Omega}_2e_{10}, \\
\tilde{\Psi}_2 =& \tilde{\Psi}_4 = \mu\rho e_3^T\tilde{\Omega}_1e_3 + \rho e_3^T\tilde{\Omega}_2e_3 + \mu\rho e_3^T\tilde{\Omega}_1e_9 + \rho e_3^T\tilde{\Omega}_2e_{10} \\
&+2\bar{\sigma}e_3^TG^TGe_3 + \bar{\sigma}\mathcal{H}(e_3^TG^TGe_9) + \bar{\sigma}\mathcal{H}(e_3^TG^TGe_{10}) \\
&-\bar{\sigma}e_9^TG^TGe_9 + \bar{\sigma}e_{10}^TG^TGe_{10} - \bar{\sigma}e_{11}^Te_{11} - \bar{\sigma}e_{12}^Te_{12} \\
&+(\rho-1)\mu e_9^T\tilde{\Omega}_1e_9 + (\rho-1)e_{10}^T\tilde{\Omega}_2e_{10},
\end{aligned}
$$

$$\chi_0 = \begin{bmatrix}e_1-e_2\\ e_1+e_2-2e_5\end{bmatrix},\ \chi_1 = \begin{bmatrix}e_2-e_3\\ e_2+e_3-2e_6\end{bmatrix},$$

$$\chi_2 = \begin{bmatrix}e_3-e_4\\ e_3+e_4-2e_7\end{bmatrix},\ \underline{\chi}_3 = \begin{bmatrix}e_1\\ \tau_1e_5\\ (\tau_2-\tau_1)e_7\end{bmatrix},\ \bar{\chi}_3 = \begin{bmatrix}e_1\\ \tau_1e_5\\ (\tau_2-\tau_1)e_6\end{bmatrix},$$

$$\chi_4 = \begin{bmatrix}e_8\\ e_1-e_2\\ e_2-e_4\end{bmatrix} \text{ and } \tilde{\mathcal{R}}_i = \begin{bmatrix}\tilde{R}_i & 0\\ 0 & 3\tilde{R}_i\end{bmatrix},\ i\in\mathcal{I}_2.$$

In that case, the gain matrices of the networked controller (5) are given by $K_1 = \tilde{K}_1X^{-1}$ and $K_2 = \tilde{K}_2X^{-1}$, and the weighting matrix of the FWMETM instant released condition (2) by $\Omega_1 = X^{-T}\tilde{\Omega}_1X^{-1}$ and $\Omega_2 = X^{-T}\tilde{\Omega}_2X^{-1}$.

Proof 1. Let us consider the following delay-dependent LKF candidate:

$$V(t) = V_1(t) + V_2(t) + V_3(t) \tag{10}$$

where $V_1(t) = x^T(t)Px(t)$, and:

$$
\begin{aligned}
V_2(t) =& \int_{t-\tau_1}^{t} x^T(s)Q_1x(s)ds + \int_{t-\tau(t)}^{t} x^T(s)Q_2x(s)ds \\
&+\tau_1\int_{-\tau_1}^{0}\int_{t+\theta}^{t}\dot{x}^T(s)R_1\dot{x}(s)dsd\theta \\
&+(\tau_2-\tau_1)\int_{-\tau_2}^{-\tau_1}\int_{t+\theta}^{t}\dot{x}^T(s)R_2\dot{x}(s)dsd\theta,
\end{aligned}
$$

$$V_3(t)=(\tau_2-\tau(t))\left(\theta^T(t)S\theta(t)+\int_{t-\tau(t)}^{t}\dot{x}^T(s)L\dot{x}(s)ds\right),$$

with $\theta(t)=\text{col}\left\{x(t),\ \int_{t-\tau_1}^{t}x(s)ds,\ \int_{t-\tau_2}^{t-\tau_1}x(s)ds\right\}$.

The LKF candidate (10) is positive if P, Q_1, Q_2, Q_3, R_1, R_2, S and L are all positive definite matrices. In this case, the closed-loop system (7) subject to the deception attack is asymptotically stable if:

$$\mathbb{E}\{\dot{V}(t)\}=\mathbb{E}\{\dot{V}_1(t)+\dot{V}_2(t)+\dot{V}_3(t)\}<0 \tag{11}$$

Let us define:

$$\zeta=\text{col}\Big\{x(t),x(t-\tau_1),x(t-\tau(t)),x(t-\tau_2),\frac{1}{\tau_1}\int_{t-\tau_1}^{t}x(s)ds,$$
$$\frac{1}{\tau(t)-\tau_1}\int_{t-\tau(t)}^{t-\tau_1}x(s)ds,\ \frac{1}{\tau_2-\tau(t)}\int_{t-\tau_2}^{t-\tau(t)}x(s)ds,$$
$$\dot{x}(t),e(t_k),e(t_{k-1}),f(x(t_k)),f(x(t_{k-1}))\Big\}$$

Yields the time-derivative of $V_1(t)$:

$$\dot{V}_1(t)=2x^T(t)P\dot{x}(t)=\zeta^T\mathcal{H}(e_1^TPe_8)\zeta \tag{12}$$

Next, the time-derivative of $V_2(t)$ is given by:

$$\begin{aligned}\dot{V}_2(t)&=\dot{x}^T(t)\big(\tau_1^2R_1+(\tau_2-\tau_1)^2R_2\big)\dot{x}(t)+x^T(t)Q_1x(t)\\&-x^T(t-\tau_1)Q_1x(t-\tau_1)-x^T(t-\tau_2)Q_2x(t-\tau_2)\\&-\tau_1\int_{t-\tau_1}^{t}\dot{x}^T(s)R_1\dot{x}(s)ds-(\tau_2-\tau_1)\int_{t-\tau_2}^{t-\tau_1}\dot{x}^T(s)R_2\dot{x}(s)ds\end{aligned} \tag{13}$$

From the extended Wirtinger inequality (Park et al., 2015), we can write:

$$-\tau_1\int_{t-\tau_1}^{t}\dot{x}^T(s)R_1\dot{x}(s)ds\le-\zeta^T\chi_0^T\mathcal{R}_1\chi_0\zeta, \tag{14}$$

$$\begin{aligned}&-(\tau_2-\tau_1)\int_{t-\tau_2}^{t-\tau_1}\dot{x}^T(s)R_2\dot{x}(s)ds\\&\le-\zeta^T\left(\frac{1}{\alpha(t)}\chi_1^T\mathcal{R}_2\chi_1-\frac{1}{1-\alpha(t)}\chi_2^T\mathcal{R}_2\chi_2\right)\zeta,\end{aligned} \tag{15}$$

with $\mathcal{R}_i=\begin{bmatrix}R_i & 0\\ 0 & 3R_i\end{bmatrix}$, $i\in\mathcal{I}_2$, $\alpha(t)=\frac{\tau(t)-\tau_1}{\tau_2-\tau_1}$, and with χ_0, χ_1 and χ_2 defined in Theorem 1.

Providing that $\begin{bmatrix}\mathcal{R}_2 & \mathcal{W}\\ * & \mathcal{R}_2\end{bmatrix}>0$ (granted by congruence from (8)), we apply the reciprocally convex approach (see Theorem 1 in (Park et al., 2011)) such that:

$$-(\tau_2-\tau_1)\int_{t-\tau_2}^{t-\tau_1}\dot{x}^T(s)R_2\dot{x}(s)ds\le\zeta^T\begin{bmatrix}\chi_1\\ \chi_2\end{bmatrix}^T\begin{bmatrix}\mathcal{R}_2 & \mathcal{W}\\ * & \mathcal{R}_2\end{bmatrix}\begin{bmatrix}\chi_1\\ \chi_2\end{bmatrix}\zeta \tag{16}$$

That is to say:

$$\dot{V}_2(t)\le\zeta^T\Phi\zeta \tag{17}$$

with $\Phi=e_1^TQ_1e_1-e_2^TQ_1e_2-e_4^TQ_2e_4+\chi_0^T\mathcal{R}_1\chi_0+e_8^T(\tau_1^2R_1+(\tau_2-\tau_1)^2R_2)e_8-\begin{bmatrix}\chi_1\\ \chi_2\end{bmatrix}^T\begin{bmatrix}\mathcal{R}_2 & \mathcal{W}\\ * & \mathcal{R}_2\end{bmatrix}\begin{bmatrix}\chi_1\\ \chi_2\end{bmatrix}$.

Now, taking the time-derivative of $V_3(t)$, we get:

$$\begin{aligned}\dot{V}_3(t)=&-\theta^T(t)S\theta(t)-\int_{t-\tau(t)}^{t}\dot{x}^T(s)L\dot{x}(s)ds\\&+(\tau_2-\tau(t))(2\theta^T(t)S\dot{\theta}(t)+\dot{x}^T(t)L\dot{x}(t))\end{aligned} \tag{18}$$

Applying Jensen's inequality, we get:

$$\dot{V}_3(t)\le\zeta^T\Xi(\tau(t))\zeta \tag{19}$$

with $\Xi(\tau(t))=-\chi_3^T\begin{bmatrix}S_{11} & S_{12} & S_{13}\\ * & S_{22} & S_{23}\\ * & * & S_{33}\end{bmatrix}\chi_3+\frac{1}{\tau_1}\begin{bmatrix}e_1\\ e_3\end{bmatrix}^T\begin{bmatrix}-L & L\\ * & -L\end{bmatrix}\begin{bmatrix}e_1\\ e_3\end{bmatrix}+(\tau_2-\tau(t))\left(\mathcal{H}\left(\chi_3^T\begin{bmatrix}S_{11} & S_{12} & S_{13}\\ * & S_{22} & S_{23}\\ * & * & S_{33}\end{bmatrix}\chi_4\right)+e_8^TLe_8\right)$,

$\chi_3=\begin{bmatrix}e_1\\ \tau_1e_5\\ (\tau(t)-\tau_1)e_6+(\tau_2-\tau(t))e_7\end{bmatrix}$ and χ_4 defined above.

From (12), (17) and (19), we can write:

$$\dot{V}(t)\le\zeta^T(\mathcal{H}(e_1^TPe_8)+\Phi+\Xi(\tau(t)))\zeta \tag{20}$$

Moreover, let us rewrite the closed-loop dynamics (7) as $\mathcal{G}(\sigma(t),t_k)\zeta=0$ with:

$$\begin{aligned}\mathcal{G}(\sigma(t),t_k)=\Big[&A\ \ 0\ \ (1-\sigma(t))B(\varsigma_1(x(t_k))K_1+\varsigma_2(x(t_k))K_2)\\&\ldots 0\ \ 0\ \ 0\ \ 0\ -I\ \ \varsigma_1(x(t_k))(1-\sigma(t))BK_1\ \ \varsigma_2(x(t_k))(1-\sigma(t))BK_2\\&\ldots\varsigma_1(f(x(t_k)))\sigma(t)BK_1\ \ \varsigma_2(f(x(t_k)))\sigma(t)BK_2\Big].\end{aligned}$$

Therefore, applying the Finsler's Lemma (Skelton et al., 1998), $\dot{V}(t)<0$ holds if there exists $\mathcal{T}\in R^{12n\times n}$ such that:

$$\zeta^T\big(\Phi+\Xi(\tau(t)+\mathcal{H}(e_1^TPe_8+\mathcal{T}\mathcal{G}(\sigma(t),t_k))\big)\zeta<0 \tag{21}$$

Then, in order to take into account the event-triggering condition (2) and the deception attack condition (6), $\forall t\in\mathbb{I}_l$, the inequality (21) is satisfied if:

$$\begin{aligned}&\zeta^T(\Phi+\Xi(\tau(t)+\mathcal{H}(e_1^TPe_8+\mathcal{T}\mathcal{G}(\sigma(t),t_k)))\zeta\\&+\sum_{i=1}^{2}\varsigma_i(x(t_k))(\rho x^T(t_{k-i+1})\Omega_ix(t_{k-i+1})-e^T(t_{k-i+1})\Omega_ie(t_{k-i+1}))\\&+\sigma(t)(x(t-\tau(t))+e(t_k))^TG^TG(x(t-\tau(t))+e(t_k))\\&+\sigma(t)(x(t-\tau(t))+e(t_{k-1}))^TG^TG(x(t-\tau(t))+e(t_{k-1}))\\&-\sigma(t)(f^T(x(t_k)f(x(t_k))-f^T(x(t_{k-1})f(x(t_{k-1})))<0\end{aligned} \tag{22}$$

Since $x(t_{k-i+1})=x(t-\tau(t))+e(t_{k-i+1})$ and $\mathbb{E}(\sigma(t))=\bar{\sigma}$, the inequality (11) is satisfied if, $\forall\zeta\neq0$:

$$\Phi+\Xi(t)+\mathcal{H}(e_1^TPe_8+\mathcal{T}\mathcal{G}(\bar{\sigma},t_k))+\Psi(\bar{\sigma},t_k)<0 \tag{23}$$

with $\Psi(\bar{\sigma},t_k)=\varsigma_1(x(t_k))\rho e_3^T\Omega_1e_3+\varsigma_2(x(t_k))\rho e_3^T\Omega_2e_3+\varsigma_1(x(t_k))\rho e_3^T\Omega_1e_9+\varsigma_2(x(t_k))\rho e_3^T\Omega_2e_{10}+2\bar{\sigma}e_3^TG^TGe_3+\bar{\sigma}\mathcal{H}(e_3^TG^TGe_9)+\bar{\sigma}\mathcal{H}(e_3^TG^TGe_{10})-\bar{\sigma}e_9^TG^TGe_9+\bar{\sigma}e_{10}^TG^TGe_{10}-\bar{\sigma}e_{11}^Te_{11}-\bar{\sigma}e_{12}^Te_{12}+(\rho-1)\varsigma_1(x(t_k))e_9^T\Omega_1e_9+(\rho-1)\varsigma_2(x(t_k))e_{10}^T\Omega_2e_{10}$.

To cope with the product $\mathcal{T}\mathcal{G}(\bar{\sigma},t_k)$ let $X\in\mathbb{R}^{n\times n}$ regular and $\mathcal{T}=[X^{-T}\ \ 0\ \ \epsilon_1X^{-T}\ \ 0\ \ldots\ 0\ \ \epsilon_2X^{-T}\ \ 0\ \ldots\ 0]^T$. Then, take the congruence of (23) by D_X and make the changes of variables $\tilde{P}=X^TPX$, $\tilde{Q}_1=X^TQ_1X$, $\tilde{Q}_2=X^TQ_2X$, $\tilde{Q}_3=X^TQ_3X$, $\tilde{R}_1=X^TR_1X$, $\tilde{R}_2=X^TR_2X$, $\tilde{S}=X^TSX$, $\tilde{L}=X^TLX$, $\tilde{\Omega}_1=X^T\Omega_1X$, $\tilde{\Omega}_2=X^T\Omega_2X$, $\tilde{\mathcal{W}}=X^T\mathcal{W}X$, $\tilde{K}_1=K_1X$ and $\tilde{K}_2=K_2X$. Finally, from the convexity of the fuzzy weighting functions (3), with $\varsigma_1(t_k)\in[0,\mu]$ and $\varsigma_2(t_k)\in[1-\mu,1]$, we obtain the LMIs of Theorem 1. □

Remark 2. The conditions of Theorem 1 are not strictly LMI because of some scalar parameters (ϵ_1 and ϵ_2). Fortunately, the search for a solution is done offline. Hence, these parameters can be tuned by grid search, as usually done in many recent studies, see e.g. (Bourahala et al., 2017; Cherifi et al., 2019; Bourahala et al., 2021).

4. ILLUSTRATIVE EXAMPLE

In order to illustrate the effectiveness of the proposed FWMETM strategy and networked controller design conditions, let us consider a fourth-order numerical example, drawn from the benchmark of a quarter-car active suspension system with 2 degrees of freedom (Wang et al., 2019), which state space model (1) is specified by:

$$A=\begin{bmatrix} 0 & 1 & 0 & -1 \\ -43.9054 & -1.1254 & 0 & 1.1254 \\ 0 & 0 & 0 & 1 \\ 374.7368 & 9.6053 & -886.9737 & -9.7333 \end{bmatrix}, B=\begin{bmatrix} 0 \\ 0.0010 \\ 0 \\ -0.0088 \end{bmatrix}$$

To show the effectiveness of the proposed FWMETM and the control design method, two cases are proposed in the sequel. In the first case, we assume that the NCS is not subject to deception attacks. Then, in the second case, we assume randomly occurring attacks.

Case 1. Suppose that there are no deception attacks occurring (i.e. $\bar{\sigma}=0$). Setting the parameters $\mu=0.01$, $\epsilon_1=10.5$, $\epsilon_2=0.2$ and $\rho=0.2$, the conditions of Theorem 1 have been solved via the Matlab LMI Toolbox and provide a maximal value of $\tau_2=59\,ms$, as well as the following sampled-data controller (5) gains matrices and the FWMETM (2) triggering weighting matrix:

$$\begin{bmatrix} K_1 \\ K_2 \end{bmatrix}=\begin{bmatrix} -55.8362 & -5.0521 & 136.3133 & 13.0104 \\ 6684.72 & 30.8227 & -15008.5 & 294.459 \end{bmatrix},$$

$$\Omega_1=10^9\times\begin{bmatrix} 2777.41 & 63.0872 & -6324.45 & -41.8167 \\ 63.0872 & 2.23814 & -145.793 & -3.49797 \\ -6324.45 & -145.793 & 14432.65 & 1.45836 \\ -41.8167 & -3.49797 & 101.458 & 8.82727 \end{bmatrix},$$

$$\Omega_2=10^9\times\begin{bmatrix} 1144.56 & 5.75108 & -2569.19 & 48.8140 \\ 5.75108 & 0.04715 & -12.9479 & 0.19008 \\ -2569.19 & -12.9479 & 5770.91 & -109.523 \\ 48.8140 & 0.19008 & -109.523 & 2.26406 \end{bmatrix}.$$

Assuming $h=10\,ms$, the allowed maximal network-induced delay is $\bar{\tau}=\tau_2-h=49\,ms$. A simulation of the designed closed-loop NCS (7) is performed with the initial condition $x_0=[\,-0.2\,0.3\,-0.3\,0.2\,]^T$, under the designed release condition (2). Fig. 2 depicts the closed-loop state trajectories, the evolution of the fuzzy weighting functions and the obtained event-triggering intervals at their release instants. The designed NCS is properly stabilized and achieved the origin in less than $30\,s$. Moreover, recall that we also aim at avoiding unnecessary transmissions in the designed NCS. Table 1 lists the Transmitted Packets Number (TPN) and the Transmission Rate (TR) obtained from the application of Theorem 1 and previous related results from the literature. We observe that, among all the tested results, Theorem 1 provides the most relaxed results. This confirms the effectiveness and the conservatism improvement of the proposed FWMETM strategy and controller design for NCS.

Table 1. Comparison of the AVI and TPN

Methods	TPN	RT
Th. 1 $(t\in[0,30], h=0.01)$	510	17.00%
(Viadero-Monasterio et al., 2022) $(t\in[0,10])$	126	18.4%
(Rouamel et al., 2021) $(t\in[0,30], h=0.01)$	756	25.22%
(Yang et al., 2021) $(t\in[0,5], h=0.01)$	176	35.20%
(Guan et al., 2018) $(t\in[0,5], h=0.01)$	207	41.40%
(Fei et al., 2019) $(t\in[0,3], h=0.005)$	253	42.20%
(Zhang et al., 2015) $(t\in[0,3], h=0.005)$	280	46.60%

Case 2. Consider now that the NCS faced randomly occurring deception attacks satisfying assumption 4 with:

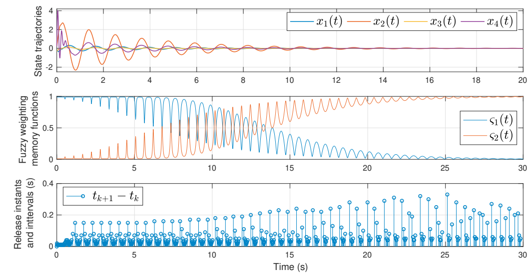

Fig. 2. States trajectories, fuzzy weighting memory functions, release instants and intervals, *Case 1.*

$$f(x(t_k))=\begin{bmatrix} \tanh(0.05x_1(t_k)) \\ -\tanh(0.1x_2(t_k)) \\ \tanh(0.05x_3(t_k)) \\ -\tanh(0.1x_4(t_k)) \end{bmatrix}, G=\begin{bmatrix} 0.05 & 0 & 0 & 0 \\ 0 & 0.1 & 0 & 0 \\ 0 & 0 & 0.05 & 0 \\ 0 & 0 & 0 & 0.1 \end{bmatrix}.$$

To show the influence of the deception attacks on the system's performances, the conditions of Theorem 1 have been solved for different values of $\bar{\sigma}$. Table 2 lists the number of packets released and the transmission rate obtained in simulation with these different values. It is to be noticed that the transmission rate increases slightly with the increase of the probability $\bar{\sigma}$. Moreover, with $\bar{\sigma}=0.3$, meaning that about 30% of the control actions are attacked, the controller (5) gains and the FWMETM (2) triggering parameters obtained from Theorem 1 are:

$$\begin{bmatrix} K_1 \\ K_2 \end{bmatrix}=\begin{bmatrix} 5103.22 & 91.0184 & -11588.6 & 4.93982 \\ 5709.68 & 124.404 & -13007.4 & -68.2397 \end{bmatrix},$$

$$\Omega_1=\begin{bmatrix} 1018.72 & 18.9115 & -2313.54 & -1.48633 \\ 18.9115 & 0.67639 & -43.5797 & -1.08490 \\ -2313.54 & -43.5797 & 5258.93 & 5.32249 \\ -1.48633 & -1.08490 & 5.32249 & 3.45823 \end{bmatrix},$$

$$\Omega_2=\begin{bmatrix} 1431.95 & 31.1386 & -3261.88 & -16.9204 \\ 31.1386 & 0.68411 & -70.9491 & -0.38993 \\ -3261.88 & -70.9491 & 7430.91 & 38.5858 \\ -16.9204 & -0.38993 & 38.5858 & 0.27179 \end{bmatrix}.$$

Table 2. Comparison of the AVI and TPN

Methods	$\bar{\sigma}=0$	$\bar{\sigma}=0.05$	$\bar{\sigma}=0.1$	$\bar{\sigma}=0.3$
TPN	510	529	531	553
RT	17.00%	17.63%	17.70%	18.43%

With the same initial conditions as in *Case 1*, Fig. 3 shows the state trajectories, the evolution of the fuzzy weighting memory functions, the release instants and intervals and the occurrence function of the deception attacks. We observe that the NCS is properly stabilized despite the occurrence of deception attacks. This confirms the effectiveness of our proposal.

5. CONCLUSION

In this paper, a fuzzy weighted memory event-triggered mechanism (FWMETM) is proposed to mitigate the network loads in sampled-data controller design for NCSs subject to network-induced delay and deception attack. The proposed triggering condition involves the information of the actual sampled-data packet, as well as the previous packets (memory), blended together through the proposed fuzzy weighting memory functions. The goal was to reduce the number of unnecessary transmissions, and so to save network bandwidth, with guaranteed closed-loop stability. Hence, based on the proposed FWMETM and on the choice of a suitable LKF, new networked state

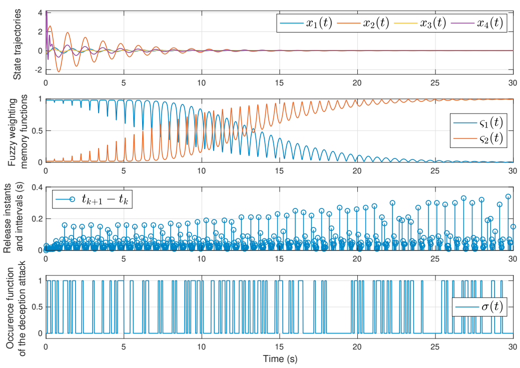

Fig. 3. States trajectories, fuzzy weighting memory functions, release instants and intervals, deception attacks, *Case2* with $\bar{\sigma} = 0.3$.

feedback sampled-data controllers design conditions have been proposed. A numerical example has been considered to illustrate the effectiveness of the proposed design conditions and the improvements raised with regard to previous related studies from the literature. Our future prospects aim at extended the present proposal to deal with nonlinear systems represented by Takagi-Sugeno models.

REFERENCES

Bourahala, F., Rouamel, M., and Guelton, K. (2021). Improved robust H_∞ stability analysis and stabilization of uncertain systems with stochastic input time-varying delays. *Optim. Contr. Appl. Methods*, 42(5), 1512–1530.

Bourahala, F., Guelton, K., Manamanni, N., and Khaber, F. (2017). Relaxed controller design conditions for Takagi–Sugeno systems with state time-varying delays. *Int. J. Fuzzy Syst.*, 19(5), 1406–1416.

Cao, J., Ding, D., Liu, J., Tian, E., Hu, S., and Xie, X. (2021). Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks. *Inf. Sci.*, 548, 69–84.

Cherifi, A., Guelton, K., Arcese, L., and Leite, V.J. (2019). Global non-quadratic d-stabilization of takagi–sugeno systems with piecewise continuous membership functions. *Appl. Math. Comput.*, 351, 23–36.

Ding, D., Wei, G., Zhang, S., Liu, Y., and Alsaadi, F.E. (2017). On scheduling of deception attacks for discrete-time networked systems equipped with attack detectors. *Neurocomputing*, 219, 99–106.

Fei, Z., Wang, X., Liu, M., and Yu, J. (2019). Reliable control for vehicle active suspension systems under event-triggered scheme with frequency range limitation. *IEEE Trans. Syst. Man Cybern.: Syst.*, 51(3), 1630–1641.

Guan, Y., Han, Q.L., Yao, H., and Ge, X. (2018). Robust event-triggered H_∞ controller design for vehicle active suspension systems. *Nonlinear Dyn.*, 94(1), 627–638.

Lopes, A.N.D., Guelton, K., Arcese, L., and Leite, V.J.S. (2021). Local sampled-data controller design for T-S fuzzy systems with saturated actuators. *IEEE Control Syst. Lett.*, 5(4), 1169–1174.

Nafir, N., Ahmida, Z., Guelton, K., Bourahala, F., and Rouamel, M. (2021). Improved robust H_∞ stability analysis and stabilisation of uncertain and disturbed networked control systems with network-induced delay and packets dropout. *Int. J. Syst. Sci.*, 52(16), 3493–3510.

Park, P., Ko, J.W., and Jeong, C. (2011). Reciprocally convex approach to stability of systems with time-varying delays. *Automatica*, 47(1), 235–238.

Park, P., Lee, W.I., and Lee, S.Y. (2015). Auxiliary function-based integral inequalities for quadratic functions and their applications to time-delay systems. *J. Frankl. Inst.*, 352(4), 1378–1396.

Qiu, L., Luo, Q., Gong, F., Li, S., and Xu, B. (2013). Stability and stabilization of networked control systems with random time delays and packet dropouts. *J. Frankl. Inst.*, 350(7), 1886–1907.

Rouamel, M., Bourahala, F., and Guelton, K. (2022). Relaxed stability analysis and sampled-data controller design for networked control systems with network-induced delays. *Trans. Inst. Meas. Control*, In press.

Rouamel, M., Bourahala, F., Lopes, A.N., Nafir, N., and Guelton, K. (2021). Mixed actual and memory data-based event-triggered H_∞ control design for networked control systems. *IFAC-PapersOnLine*, 54(4), 80–85.

Rouamel, M., Gherbi, S., and Bourahala, F. (2020). Robust stability and stabilization of networked control systems with stochastic time-varying network-induced delays. *Trans. Inst. Meas. Control*, 42(10), 1782–1796.

Skelton, R., Iwasaki, T., and Grigoriadis, K. (1998). *A unified algebraic approach to linear control design.* Taylor and Francis, London.

Sun, X., Gu, Z., Yang, F., and Yan, S. (2021). Memory-event-trigger-based secure control of cloud-aided active suspension systems against deception attacks. *Inf. Sci.*, 543, 1–17.

Tian, E., Wang, K., Zhao, X., Shen, S., and Liu, J. (2019). An improved memory-event-triggered control for networked control systems. *J. Frankl. Inst.*, 356(13), 7210–7223.

Viadero-Monasterio, F., Boada, B., Boada, M., and Díaz, V. (2022). H_∞ dynamic output feedback control for a networked control active suspension system under actuator faults. *Mech. Syst. Signal Process.*, 162, 108050.

Wang, G., Chadli, M., Chen, H., and Zhou, Z. (2019). Event-triggered control for active vehicle suspension systems with network-induced delays. *J. Frankl. Inst.*, 356(1), 147–172.

Wang, K., Tian, E., Liu, J., Wei, L., and Yue, D. (2020). Resilient control of networked control systems under deception attacks: a memory-event-triggered communication scheme. *Int. J. Robust Nonlinear Control*, 30(4), 1534–1548.

Yang, C., Xia, J., Park, J.H., Shen, H., and Wang, J. (2021). Sliding mode control for uncertain active vehicle suspension systems: an event-triggered control scheme. *Nonlinear Dyn.*, 103(4), 3209–3221.

Yue, D., Tian, E., and Han, Q.L. (2012). A delay system method for designing event-triggered controllers of networked control systems. *IEEE Trans. Automat. Contr.*, 58(2), 475–481.

Zhang, D., Han, Q.L., and Jia, X. (2015). Network-based output tracking control for T–S fuzzy systems using an event-triggered communication scheme. *Fuzzy Sets syst*, 273, 26–48.

Zhang, L. and Guo, G. (2021). Observer-based adaptive event-triggered sliding mode control of saturated nonlinear networked systems with cyber-attacks. *Inf. Sci.*, 543, 180–201.