European Journal of Control 69 (2023) 100765

Contents lists available at ScienceDirect

European Journal of Control

journal homepage: www.elsevier.com/locate/ejcon

Fixed-time event-triggered control under denial-of-service attacks

Kallol Chatterjee[a], Vijay K. Singh[a], Parijat Prasun[a], Shyam Kamal[a], Sandip Ghosh[a], Thach N. Dinh[b,*]

[a] Department of Electrical Engineering, Indian Institute of Technology (BHU) Varanasi, Varanasi, U.P. 221005, India
[b] Conservatoire National des Arts et Métiers (CNAM), Cedric-Lab, 292 rue St-Martin, 75141 Paris Cedex 03, France

ARTICLE INFO

Article history:
Received 3 June 2022
Revised 23 September 2022
Accepted 14 December 2022
Available online 22 December 2022

Recommended by Prof. T Parisini

Keywords:
Fixed-time stability
Denial-of-service
Event-triggered control

ABSTRACT

In this article, fixed-time event-triggered control is designed for a networked system under denial-of-service (DoS) attacks. At first, fixed-time input-to-state stability (ISS) analysis without DoS is analyzed. Then, fixed-time ISS under DoS is examined under the same control law. Sufficient conditions for the frequency of DoS attacks and the time duration of DoS attacks are obtained so that the closed-loop system retains the fixed-time ISS. A numerical example is also given to demonstrate the outcomes of the proposed methodology.

1. Introduction

The networked control system is omnipresent nowadays, be it manufacturing industries, autonomous vehicles, power transmission, distribution networks, etc. In many networked control systems, the communication channel between the controller, actuator and sensor is open. With the increased use of such systems, the concern for the safety and security of the network is essential for smooth operation [29]. Recently, this area has come under the scope of many researchers [12,22]. Many control system researchers have also explored this problem from their perspective [21,28]. As far as network security is concerned, one of the important issues is to know about different types of attacks which can harm the network and mitigate their effects to a large extent [16,27]. However, there are many other vulnerabilities in the network, which are exploited by the cyber attackers, causing interruptions in network communication. The specific term for such situations is called denial-of-service (DoS) [2,24]. The attackers employing DoS attacks usually have limited information of the sensor data and the control input. So, they try to interrupt the communication in the network and prevent the continuous transmission of the control input signal to the plant. This may give rise to the closed-loop system instability due to denied controller to actuator communication channel and sensor to the controller communication channel [17]. There are various models which are used to represent DoS attacks over the communication network, such as the probabilistic packet drop model, general attacks model, etc. The various classifications of DoS attacks in literature are random attacks, trivial attacks, protocol-aware jamming attacks, periodic attacks, etc. [19,25]. In [7] authors have modeled DoS attacks using pulse-width-modulated signal. Here they have identified the attributes, such as maximum on/off cycles of the DoS signal.

Stability analysis under DoS becomes an essential task since under DoS attacks, systems operate in the open-loop with the control input similar to what was transmitted just before the occurrence of DoS attacks [9,26]. The sampling-based state feedback control is proposed in Dolk et al. [5] for the linear networked control systems under the existence of DoS attacks. In this paper, the authors adopted the idea of the event triggering technique in such a way that the networked system under control remains exponentially input-to-state stable. To ensure input-to-output stability, the output-based resilient control methods are proposed in Feng and Tesi [8], where the obtained closed-loop system is nonlinear Lipschitz. In [4], the global exponential stability is studied while DoS attacks over the communication channel of the networked control system. This type of stability can be quantified in terms of the rate of convergence, but the solution approaches the equilibrium point after a very large time which is not finite [20].

One of the prime objectives under the presence of DoS attacks is to know whether the closed-loop stability is preserved or not. The input-to-state stabilizing control under the presence of DoS

[*] Corresponding author.
E-mail addresses: kallolchatterjee.eee20@iitbhu.ac.in (K. Chatterjee), vijaykumarsingh.rs.eee19@iitbhu.ac.in (V.K. Singh), parijatprasun.rs.eee19@iitbhu.ac.in (P. Prasun), shyamkamal.eee@iitbhu.ac.in (S. Kamal), sghosh.eee@iitbhu.ac.in (S. Ghosh), ngoc-thach.dinh@lecnam.net (T.N. Dinh).

https://doi.org/10.1016/j.ejcon.2022.100765

attacks is discussed in De Persis and Tesi [3]. In this article, they studied the duration of DoS attacks as well as the frequency of DoS attacks so that the input-to-state stability of the closed-loop system is preserved. In [30], authors have discussed the mean square exponential stability of a stochastic network system under the impact of an aperiodic DoS attacks. Here, a secure controller is proposed by designing an observer-based event triggering mechanism. In [6], the authors have analyzed the worst-case scenario under which the closed-loop networked control system remains finite-time stable considering the successful launch of DoS attacks from an attacker. In finite-time stability, the solution converges to the equilibrium point with a constant velocity making the time of convergence finite [1]. However, the time of convergence is also very large for the large initial condition since the time of convergence depends on the initial condition [13]. To overcome this problem, the concept of fixed-time stability was proposed in Polyakov [18]. In this, the time of convergence is bounded by a maximum time which is independent of the initial condition. Hence, regardless of any initial condition, no matter how large, the solution will always converge within some fixed-time, which is known a priori [10].

Motivated by the aforementioned observations, in this paper, the main aim is to look over the susceptibility of fixed-time ISS of closed-loop networked systems under the presence of DoS attacks. The sufficient conditions on DoS attacks frequency and time-duration are also obtained in an attempt to preserve the fixed-time ISS of the closed-loop network system. The main contributions of this work are twofold:

(1) A fixed-time Zeno-free event-triggered control mechanism have been designed for nonlinear systems without considering the DoS attack. The event-triggering conditions are appropriately designed such that it constrains the system trajectory to origin in fixed-time irrespective of the initial conditions and the inter-event times of the controller are bounded away from zero to avoid Zeno behavior.

(2) The characterization of frequency and duration of the DoS attack is obtained under which the fixed-time stability of the closed-loop system preserved. Further, we relate the fixed-time stability properties to the frequency and duration of DoS ON/OFF transitions.

In this article, we analyse the fixed-time input to state stability of a closed-loop networked system under the denial-of-service attack by utilizing an event-triggered mechanism. To be more precise, the determination of the sufficient conditions for which the preservation of the fixed-time input to state stability under the DoS attack can be claimed is of prime focus. To the best of author's knowledge, there is no work addressing the above-mentioned issues. The most recent work which addresses the issue of stability preservation is of Doostmohammadian and Meskin [6], which focusses on the finite-time input to state stability under the DoS attack. Finally, the validity of the proposed stabilization scheme is demonstrated with a numerical example through a simulation study.

This article is organized as follows. Notations and definitions are briefly introduced in Section 2. The main results are presented in Section 3. A numerical example with simulation results is shown in Section 4, followed by the concluding remarks and future scope in Section 5.

2. Notations and preliminaries

The set of all non-negative integers and the set of all positive integers are denoted by $\mathbb{N}_{\geq 0}$ and $\mathbb{N}_{>0}$ respectively. $\mathbb{R}$ represents the field of all numbers which are real and $\mathbb{R}_{\geq 0}$ is the set of all real numbers which are non-negative. $\mathbb{R}^n$ is the set of all n-dimensional vector space over the field $\mathbb{R}$. The absolute value of a scalar variable is represented by $|\cdot|$ and 2-norm or the Euclidean norm of a finite-dimensional vector of appropriate dimension is denoted by $\|\cdot\|$. $(\cdot)^\top$ denotes the transpose.

First of all, consider a nonlinear dynamical system of the form

$$\dot{z} = \mathcal{F}(z(t), u(t)), \quad z(0) = z_0 \tag{1}$$

where, $z(t) \in \mathbb{R}^n$ denotes the system state vector and $u(t) \in \mathbb{R}^m$ system input vector. The control law is taken as $u(t) = \phi(z(t), \xi(t))$, where $\xi(t)$ denotes the error signal occurs due to sampling.

The closed-loop system can be rewritten as:

$$\dot{z} = \mathcal{F}(z(t), \phi(z(t), \xi(t)) = \mathcal{G}(z(t), \xi(t)), \; z(0) = z_0 \tag{2}$$

Definition 1 ([11]). The system (2) is said to be *finite-time ISS* with respect to the input $\xi(t)$ if for every input $\xi(t) \in \mathbb{R}^n$ and for all initial conditions $z_0 \in \mathbb{R}^n$ such that $\|\xi(t)\|_\infty < \delta$, the following satisfies

$$\|z(t)\| \leq \beta(\|z_0\|, t) + \bar{\gamma}\left(\sup_{0 \leq \tau \leq t} \|\xi(\tau)\|\right) \tag{3}$$

where $\bar{\gamma}$ and β are class $\mathcal{K}_\infty$ function[1] and $\mathcal{KL}$ function[2] respectively with $\beta(\|z_0\|, t) = 0$ for all $t \geq T$ where T is a continuous function of z_0.

Definition 2 ([15]). The system (2) is said to be *fixed-time ISS* if it is finite-time ISS and $\sup_{z_0 \in \mathbb{R}_{\geq 0}} T < +\infty$.

A continuously differentiable function $V : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ is said to be an ISS-Lyapunov function for the closed-loop system (2), if for all $z \in \mathbb{R}^n$

$$\psi_1(\|z\|) \leq V(z) \leq \psi_2(\|z\|) \tag{4}$$

$$\dot{V}(z(t), \xi(t)) \leq -\psi_3(\|z(t)\|) + \gamma(\|\xi(t)\|) \tag{5}$$

where, ψ_1, ψ_2, ψ_3 and γ are class $\mathcal{K}_\infty$ functions.

Since, $-\psi_3(\|z(t)\|) \leq -\psi_3(\psi_2^{-1}(V(z(t))))$ and $\psi_3(\psi_2^{-1}(z(t))) = \psi(z(t))$ then it can be said,

$$\dot{V}(z(t), \xi(t)) \leq -\psi(V(z(t))) + \gamma(\|\xi(t)\|) \tag{6}$$

Definition 3 ([11]). A continuous function V is said to be a *finite-time ISS-Lyapunov function* for the closed-loop system (2) if it is an ISS-Lyapunov function satisfying (4) and $\psi(V(z(t)))$ is of the form $cV^a(z(t))$ in (6), where $a \in (0, 1)$ i.e.,

$$\dot{V}(z(t), \xi(t)) \leq -cV^a(z(t)) + \gamma(\|\xi(t)\|) \tag{7}$$

$\forall z \in \mathbb{R}^n$ with, $c > 0$ and $\gamma \in \mathcal{K}_\infty$.

Definition 4 ([15]). A continuous function V is said to be a *fixed-time ISS-Lyapunov function* for the closed-loop system (2) if it is an ISS-Lyapunov function satisfying (4) and $\psi(V(z(t)))$ is of the form $c_1V^a(z(t)) + c_2V^b(z(t))$ in (6) where $a \in (0, 1)$ and $b \in (1, \infty)$ i.e.,

$$\dot{V}(z(t), \xi(t)) \leq -c_1V^a(z(t)) - c_2V^b(z(t)) + \gamma(\|\xi(t)\|) \tag{8}$$

$\forall z \in \mathbb{R}^n$ with, $c_1 > 0, c_2 > 0$ and $\gamma \in \mathcal{K}_\infty$.

The block diagram of the networked control system under consideration is shown in Fig. 1, where the transmission of signals between sensor to controller and controller to actuator is done through a communication network.

[1] A continuous function $\bar{\gamma} : [0, \infty) \to [0, \infty)$ is called a class $\mathcal{K}_\infty$ function if it purely increasing, $\bar{\gamma}(0) = 0$ and $\bar{\gamma}(s) \to \infty$ as $s \to \infty$.

[2] A continuous function $\beta : [0, a) \times [0, \infty) \to [0, \infty)$ is called as class $\mathcal{KL}$ function if, for all specified value of s, $\beta(r, s)$ is belongs to class $\mathcal{K}$ and for all specified value of r, $\beta(r, s) \to 0$ as $s \to \infty$.

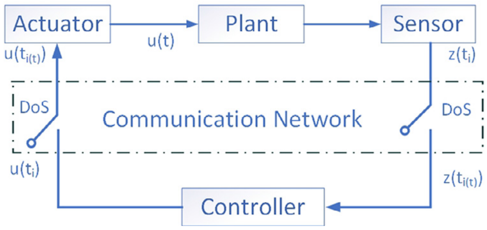

Fig. 1. Block-diagram of the networked control system under DoS attacks.

3. Main results

3.1. Fixed-time ISS without DoS attacks

In the following section, we propose an fixed-time ISS event triggering mechanism for the system (1) without considering DoS attacks.

Assumption 1. An ISS-Lyapunov function $V:\mathbb{R}^n \to \mathbb{R}_{\geq 0}$ exists for the system (2), which satisfies (8) for a given constants $a \in (0,1), b \in (1,\infty), c_1 > 0, c_2 > 0$ and class $\mathcal{K}_\infty$ functions ψ, γ.

Assumption 2. For $z \in \mathbb{R}^n$, there exist μ_1 and $\mu_2 > 0$ such that $\gamma_1((\|z\|)) \leq \mu_1 \psi_1^a(\|z\|) + \mu_2 \psi_1^b(\|z\|)$ where ψ_1, ψ_2, γ_1 are $\mathcal{K}_\infty$ functions and $\gamma_1(\|z\|) > \gamma(\|z\|)$.

Remark 1. The above assumption is based on the limiting condition of the difference between $z(t)$ and $z(t_i)$. This assumption satisfies that the error signal is within some limit. This makes the interevent value of the state $(z(t_i))$ to track the actual value of the state $(z(t))$.

Taking the above assumptions into consideration, let $\gamma_1((\|z\|)) = \gamma(4(\|z\|))$, the following event triggering rule is proposed as

$$\begin{aligned} t_{i+1} = \inf\{t > t_i | \gamma(4\|\xi(t)\|) > c_1(1-\epsilon)V^a(z(t)) \\ +c_2(1-\epsilon)V^b(z(t))\} \end{aligned} \tag{9}$$

with $\epsilon \in (0,1)$ is called triggering parameter, $\xi(t) = z(t_i) - z(t)$, $c_1 > 0$, $c_2 > 0$ and $V(z(t))$ satisfies (8).

Theorem 1. *The system (1) under the proposed event-triggering rule (9) and with input $u(t) = \phi(z(t), \xi(t))\ \forall\ t \in [t_i, t_{i+1})$ is fixed-time ISS. Moreover, the Lyapunov function satisfies the following inequalities*

$$\begin{aligned} & V(z(t))^{1-a} \leq V(z(t_i))^{1-a} - \Omega_1(1-a)(t-t_i) \\ & \quad \text{for } V(z(t)) \leq 1 \\ & \quad V(z(t))^{1-b} \geq V(z(t_i))^{1-b} - \Omega_2(1-b)(t-t_i) \\ & \quad \text{for } V(z(t)) > 1 \end{aligned} \tag{10}$$

where, $\Omega_1 = c_1\epsilon, \Omega_2 = c_2\epsilon$ and $t_i < t < t_{i+1}$.

Proof. Considering Assumption 1, we get $\dot{V}(z(t), \xi(t)) \leq -c_1 V^a(z(t)) - c_2 V^b(z(t)) + \gamma(\|\xi(t)\|)$. Now, employing event triggering rule (9), for $t_i < t < t_{i+1}$, we have $\gamma(4\|\xi(t)\|) \leq c_1(1-\epsilon)V^a(z(t)) + c_2(1-\epsilon)V^b(z(t))$.

As we know γ is a $\mathcal{K}_\infty$ function, we get

$$\begin{aligned} \dot{V}(z(t), \xi(t)) &\leq -c_1 V^a(z(t)) - c_2 V^b(z(t)) \\ &\quad + c_1(1-\epsilon)V^a(z(t)) + c_2(1-\epsilon)V^b(z(t)) \\ &\leq -c_1\epsilon V^a(z(t)) - c_2\epsilon V^b(z(t)) \end{aligned} \tag{11}$$

So, from (11) we can say that system (2) is fixed-time ISS.

Furthermore, from (11), we can note that $\dot{V}(z(t), \xi(t)) \leq -c_1\epsilon V^a(z(t))$ if $V(z(t)) \leq 1$ and $\dot{V}(z(t), \xi(t)) \leq -c_2\epsilon V^b(z(t))$ if $V(z(t)) > 1$.

So, for $V(z(t)) \leq 1$ it follows:

$$\int_{V(z(t_i))}^{V(z(t))} \frac{dV}{V^a} \leq \int_{t_i}^{t} -c_1 \qquad \epsilon dt$$

$$\frac{V(z(t))^{1-a} - V(z(t_i))^{1-a}}{1-a} \leq -c_1\epsilon(t-t_i)$$

Similarly, for $V(z(t)) > 1$ it follows:

$$\int_{V(z(t_i))}^{V(z(t))} \frac{dV}{V^b} \leq \int_{t_i}^{t} -c_2 \qquad \epsilon dt$$

$$\frac{V(z(t))^{1-b} - V(z(t_i))^{1-b}}{1-b} \leq -c_2\epsilon(t-t_i)$$

For $V(z(t)) < 1$, $V(z(t))^{1-a} \leq V(z(t_i))^{1-a} - \Omega_1(1-a)(t-t_i)$.

Since $a < 1$, so from (10) we can conclude $V(z(t)) < V(z(t_i))$.

Similarly, for $b > 1$ we can say that $V(z(t)) < V(z(t_i))$. □

Remark 2. The event-triggered mechanism (9) is almost always Zeno free, since for $t_i < t < t_i + 1$ we have $\gamma(4\|\xi(t)\|) > c_1(1-\epsilon)V^a(z(t)) + c_2(1-\epsilon)V^b(z(t))$. It is known that any event-triggered mechanism for which error is restricted to satisfy $\gamma(\|\xi\|) \leq K\chi(z)$ is Zeno free wherever γ and χ^{-1} function are Lipschitz [23]. Since the functions γ, V^{-a} and V^{-b} are Lipschitz almost everywhere, the event triggering mechanism (9) does not show Zeno behavior almost everywhere.

3.2. Fixed-time stability under DoS attacks

Here, we have discussed the event-triggered fixed-time ISS under DoS attacks for the considered networked control system shown in Fig. 1. At the beginning, modeling of DoS is carried out along with some sampling scheme under the event-triggered mechanism to ensure the fixed-time ISS. The DoS occurrence's time sequences are represented by $\{\chi_n\}_{n\in\mathbb{N}_0}$. The time duration of nth DoS attacks is represented by $\tau_{n\in\mathbb{R}_0}$ for which communication is interrupted. So, the nth DoS time interval is denoted by $H_n := \chi_n \cup [\chi_n, \chi_n + \tau_n)$, which has a length $\tau_{n\in\mathbb{R}_{\geq 0}}$. In the lack of communication due to DoS, the actuator produces the input signal which was received just before the DoS occurrence.

Now, in the presence of DoS input is generated based on the last updated control signal. If, $t, \iota \in \mathbb{R}_{\geq 0}$ with $t \geq \iota$ let's $s(\iota, t) := \cup_{n\in\mathbb{N}_0} H_n \cap [\iota, t]$ as the set of time instants for which communication is interrupted and $T(\iota, t) := [\iota, t] \backslash s(t)$ as the set of time instants for which communication is allowed. Similarly, the control input applied to the plant represented as $u(t) = \phi(z(t), \xi(t))$ where for every $t \in \mathbb{R}_{\geq 0}$, $i(t)$ denotes the latest successful control update i.e.

$$i(t) := \begin{cases} -1 & \text{if } \ T(\iota, t) = 0 \\ \sup\{i \in \mathbb{N}_0 | t_i \in T(\iota, t)\}, & \text{otherwise} \end{cases}$$

The main aim here is to obtain the condition on DoS frequency in such a manner that system (2) can withstand before fixed-time stability lost. The following assumptions are made on DoS frequency and DoS duration through the time interval $[\iota, t)$.

Assumption 3 (DoS Frequency)**.** There exist $\tau_D \in [0, \infty)$ and $\eta \in [0, \infty)$ in such a way

$$n(t) \leq \eta + \frac{t}{\tau_D}, \qquad \forall t \geq 0 \tag{12}$$

here, $n(t)$ and τ_D represents the count of OFF/ON transitions and the bound on average dwell-time respectively. So the frequency of OFF/ON DoS transitions can be upper bounded by $\frac{1}{\tau_D}$.

Assumption 4 (DoS Time-Duration)**.** There exist $\varkappa \in \mathbb{R}_{\geq 0}$ and $T > 1$ in such a way

$$|s(t)| \leq \varkappa + \frac{t}{T}, \qquad \forall t \geq 0 \tag{13}$$

where $\frac{t}{T}$ represents the average DoS time duration.

Taking Assumptions 1–4 into consideration, the following event triggering rule is proposed.

Case 1. t_i is not in DoS attacks interval, then

$$\begin{aligned} t_{i+1} = \inf\{&t > t_i | \gamma(4\|\xi(t)\|) > c_1(1-\epsilon)V^a(z(t)) \\ &+ c_2(1-\epsilon)V^b(z(t))\} \end{aligned} \tag{14}$$

where $\epsilon \in (0,1)$ and $\xi(t) = z(t_i) - z(t)$.

Case 2. t_i is in DoS attacks interval, then

$$t_{i+1} = t_i + \Delta_i \tag{15}$$

where Δ_i represents the inter-event interval such that $\Delta_1 \le \Delta_i \le \Delta_2$, here $\Delta_1 > 0$ is lower bound and $\Delta_2 > 0$ is the upper bound of Δ_i.

Remark 3. Zeno phenomenon is referred as infinite numbers of discrete transition in a finite interval of time [14]. So, study of Zeno-free case is very important for event-triggering and DoS attack case. Here, the event-triggering mechanism defined by Case 1 and Case 2 does not show Zeno behavior almost every point. Since the sampling during DoS attacks [Case 2] is lower bounded by $\Delta_1 > 0$. This along with the Remark 1 imply that the event-triggering mechanism is Zeno-free almost everywhere.

Lemma 1. *The system (1) with control law $u(t) = \phi(z(t_{i(t)}))\ \forall\ t \in [t_i, t_i + 1)$ and if t_i is in DoS attacks interval then under the proposed event triggering rule (15), it follows*

For $V(z(t)) \le 1$

$$V(z(t))^{1-a} \le V(z(t_{i(t_i)+1}))^{1-a} + (1-a)\Omega_3(t - t_{i(t_i)+1}) \tag{16}$$

and for $V(z(t)) > 1$

$$V(z(t))^{1-b} \ge V(z(t_{i(t_i)+1}))^{1-b} + (1-b)\Omega_4(t - t_{i(t_i)+1}) \tag{17}$$

where $t_{i(t_i)+1}$ represents the first sampling time instant that can be possible and in the DoS time interval, $\Omega_3 = c_1(1-\epsilon) + 2\mu_1$, $\Omega_4 = c_2(1-\epsilon) + 2\mu_2$, $t_{i(t_i)+1} < t < t_{i+1}$ and V satisfy Assumption 1.

Proof. Let a successful data communication event instant $i(t_i)$ take place before t_i which is in DoS attacks interval and consider the Eq. (15), it follows:

$$\begin{aligned} \|\xi(t)\| \le \frac{1}{4}\gamma^{-1}(c_1(1-\epsilon)V^a(z(t)) + c_2(1-\epsilon)V^b(z(t))), \\ t_{i(t_i)} \le t \le t_{i(t)+1} \end{aligned}$$

From the continuity of Lyapunov function V, $z(t)$ and $\xi(t)$ at $t_{i(t_i)+1}$ we can write:

$$\begin{aligned} \|z(t_{i(t_i)})\| &\le \|z(t_{i(t_i)+1})\| + \|\xi(t_{i(t_i)+1})\| \\ &\le \|z(t_{i(t_i)+1})\| + \frac{1}{4}\gamma^{-1}(c_1(1-\epsilon)V^a(z(t_{i(t_i)+1})) \\ &\quad + c_2(1-\epsilon)V^b(z(t_{i(t_i)+1}))) \\ &\le \frac{1}{4}\gamma^{-1}(\mu_1 V^a(z(t_{i(t_i)+1})) + \mu_2 V^b(z(t_{i(t_i)+1}))) \\ &\quad + \frac{1}{4}\gamma^{-1}(c_1(1-\epsilon)V^a(z(t_{i(t_i)+1})) \\ &\quad + c_2(1-\epsilon)V^b(z(t_{i(t_i)+1}))) \end{aligned} \tag{18}$$

Since $\gamma \in \mathcal{K}_\infty$ function and for any $p, q \ge 0$ we know $\gamma(p+q) \le \gamma(2p) + \gamma(2q)$, for $\xi(t) = z(t_{i(t_i)}) - z(t)$ in time interval $t_{i(t_i)} \le t \le t_{i(t_i)+1}$, we get

$$\begin{aligned} \gamma(\|\xi(t)\|) &\le \gamma(2\|z(t_{i(t_i)})\|) + \gamma(2\|z(t)\|) \\ &\le ((c_1(1-\epsilon) + \mu_1)V^a(z(t_{i(t_i)+1})) \\ &\quad + (c_2(1-\epsilon) + \mu_2)V^b(z(t_{i(t_i)+1})) \\ &\quad + \mu_1 V^a(z(t)) + \mu_2 V^b(z(t))) \end{aligned}$$

Now for $V(z(t)) \le 1$ we can say that,

$$\begin{aligned} \dot V(z(t)) &\le ((c_1(1-\epsilon) + \mu_1)V^a(z(t_{i(t_i)+1})) + (\mu_1 - \epsilon)V^a(z(t)) \\ &\le \Omega_3 \max\{V^a(z(t_{i(t_i)+1})), V^a(z(t))\} \end{aligned} \tag{19}$$

and for $V(z(t)) > 1$ we can say that,

$$\begin{aligned} \dot V(z(t)) &\le ((c_2(1-\epsilon) + \mu_2)V^b(z(t_{i(t_i)+1})) + (\mu_2 - \epsilon)V^b(z(t)) \\ &\le \Omega_4 \max\left\{V^b(z(t_{i(t_i)+1})), V^b(z(t))\right\} \end{aligned} \tag{20}$$

for $t_{i(t_i)+1} \le t < t_{i+1}$. Hence, to solve the differential Eqs. (19) and (20), we consider $\dot\nu(t) = \Omega_3 \max\{V^a(z(t_{i(t_i)+1})), V^a(z(t))\}$ for $t_{i(t_i)+1} \le t < t_{i+1}$ with $\nu(t_{i(t_i)+1}) = V(z(t_{i(t_i)+1}))$ as the initial condition, we obtain

$$\nu(t) = (\nu^{1-a}(t_{i(t_i)+1}) + \Omega_3(t - t_{i(t_i)+1}))^{\frac{1}{1-a}}$$

from comparison lemma, one can note that $V(t) \le \nu(t)$ which further results to (16). Similarly for the case of $V(z(t)) > 1$ we can also calculate:

$$\begin{aligned} V(t) &\le \left(V^{1-b}(t_{i(t_i)+1}) + \Omega_4(t - t_{i(t_i)+1})\right)^{\frac{1}{1-b}} \\ V(t)^{1-b} &\ge \left(V^{1-b}(t_{i(t_i)+1}) + \Omega_4(t - t_{i(t_i)+1})\right) \\ V(t)^{1-b} &\ge \left(V^{1-b}(t_{i(t_i)+1}) + (1-b)\Omega_4(t - t_{i(t_i)+1})\right) \end{aligned}$$

□

Remark 4. Lemma 1 determines the Lyapunov function's divergence rate. When the DoS is present and there is no successful updation of control input, the Lyapunov function can rise, the rate of which is upper bounded by (16) and (17).

Assume $\lambda(t)$ denotes the union of the time-intervals where $V(z(t))$ may grow. Now, define $\lambda^c(t) = [0, t)\backslash\lambda(t)$ where $\lambda^c(t)$ is the complement of $\lambda(t)$ in $[0, t)$. Taking Assumptions 3 and 4 into consideration, we can obtain [4]:

$$|\lambda(t)| \le \varkappa + \frac{t}{T} + \Delta_2\left(\eta + \frac{t}{\tau_D}\right) \tag{21}$$

From Theorem 1 and Lemma 1, we also obtain following using (10), (16) and (17): for $V(z(t)) \le 1$

$$V^{1-a}(z(t)) \le V_0^{1-a} + (1-a)(\Omega_3|\lambda(t)| - \Omega_1|\lambda^c(t)|) \tag{22}$$

and for $V(z(t)) > 1$

$$V^{1-b}(z(t)) \ge V_0^{1-b} + (1-b)(\Omega_4|\lambda(t)| - \Omega_2|\lambda^c(t)|) \tag{23}$$

From the obtained Eqs. (22) and (23), we can see that Lyapunov function may increase due to DoS terms, which causes the instability of the system.

The main aim here is to give the conditions on DoS frequency as well as time duration of DoS attacks in such a way that the system (2) remains fixed time input-to-state stable.

Theorem 2. *The system (1) under the proposed event triggering rule Case 1 and Case 2, input $u(t) = \phi(z(t_{i(t)}), \xi(t))$ and with Assumptions 2–4 under DoS attacks remains fixed time ISS, if the following conditions satisfy:*

$$\begin{aligned} \frac{1}{T} + \frac{\Delta_2}{\tau_D} &< \frac{c_1\epsilon}{c_1 + 2\mu_1} \\ \frac{1}{T} + \frac{\Delta_2}{\tau_D} &< \frac{c_2\epsilon}{c_2 + 2\mu_2} \end{aligned} \tag{24}$$

Proof. Consider the Eq. (21), from which we can obtain

$$\begin{aligned} \Omega_3|\lambda(t)| - \Omega_1|\lambda^c(t)| &= (c_1 + 2\mu_1)(\varkappa + \Delta_2\eta) \\ &+ t\left(\left(\frac{1}{T} + \frac{\Delta_2}{\tau_D}\right)(c_1 + 2\mu_1) - c_1\epsilon\right) = \rho_1 - \zeta_1 t \end{aligned}$$

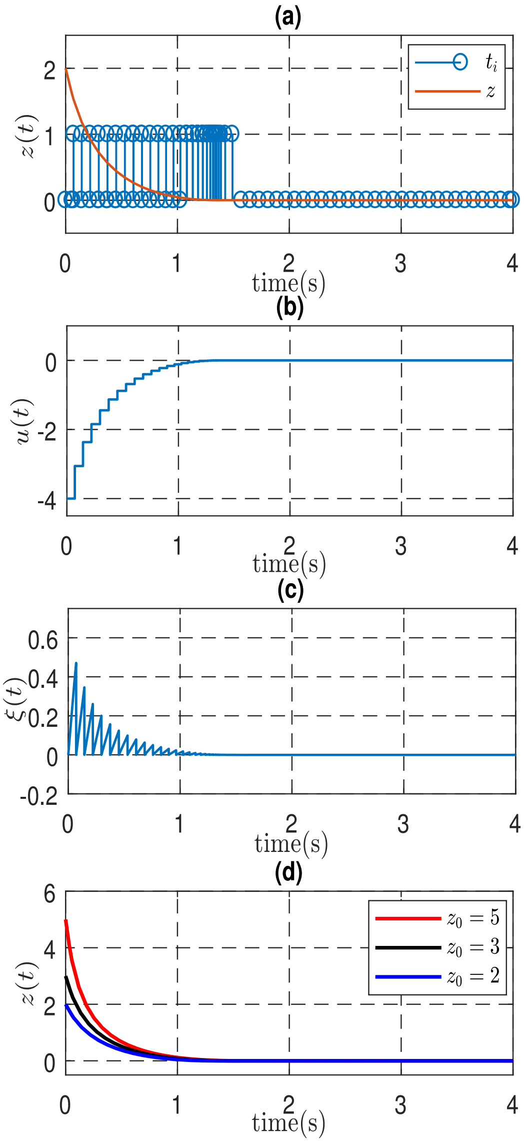

Fig. 2. (**a**) State evolution without DoS for $z_0 = 2$, where Blue bars are event triggering instances, (**b**) $u(t)$ without DoS, (**c**) $\xi(t)$ without DoS, (**d**) State evolution without DoS for different initial conditions (z_0). From the obtained result we can conclude that system (26) is fixed-time ISS with $T_{\max} = 8.75$ s.

$$\Omega_4|\lambda(t)| - \Omega_2|\lambda^c(t)| = (c_2 + 2\mu_2)(\varkappa + \Delta_2\eta) + t\left(\left(\frac{1}{T} + \frac{\Delta_2}{\tau_D}\right)(c_2 + 2\mu_2) - c_2\epsilon\right) = \rho_2 - \zeta_2 t \tag{25}$$

where,

$$\zeta_1 := c_1\epsilon - \left(\frac{1}{T} + \frac{\Delta_2}{\tau_D}\right)(c_1 + 2\mu_1)$$
$$\rho_1 := (c_1 + 2\mu_1)(\varkappa + \Delta_2\eta)$$
$$\zeta_2 := c_2\epsilon - \left(\frac{1}{T} + \frac{\Delta_2}{\tau_D}\right)(c_2 + 2\mu_2)$$
$$\rho_2 := (c_2 + 2\mu_2)(\varkappa + \Delta_2\eta)$$

Now for $V(z(t)) > 1$ we can write

$$V^{1-b}(z(t)) \geq V_0^{1-b} + (1-b)(\rho_2 - \zeta_2 t)$$

So,

$$V_0^{1-b} + (1-b)(\rho_2 - \zeta_2 t) \leq 1$$

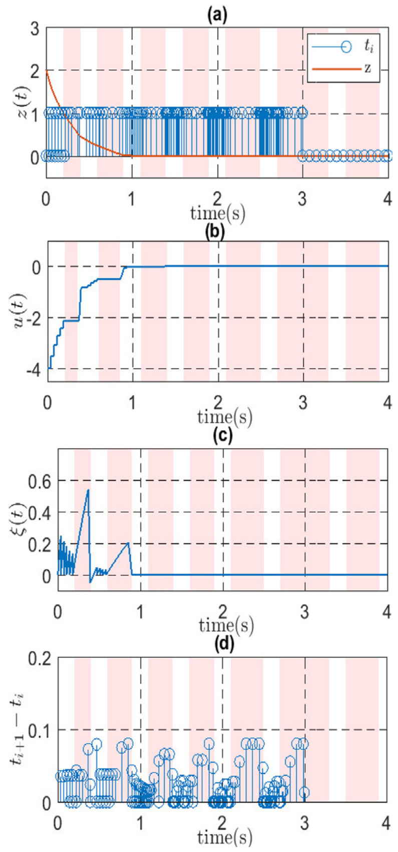

Fig. 3. (**a**) State evolution with DoS for $z_0 = 2$, where Blue bars are event triggering instances and vertical red stripes are time intervals of DoS, (**b**) $u(t)$ with DoS, (**c**) $\xi(t)$ with DoS, (**d**) Inter-event interval with DoS. From the obtained result we can conclude that system (26) remains fixed-time ISS with 75% DoS. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

$$(V_0^{1-b} - 1) \leq (b-1)(\rho_2 - \zeta_2 t)$$
$$\frac{(V_0^{1-b} - 1)}{b-1} \leq (\rho_2 - \zeta_2 t)$$
$$t \leq \frac{\rho_2}{\zeta_2} + \frac{(V_0^{1-b} - 1)}{(b-1)\zeta_2}$$

Since $V_0^{1-b} < 1$, for $t \geq \frac{\rho_2}{\zeta_2} + \frac{1}{(b-1)\zeta_2}$ we can always say that, $V(z(t)) \leq 1$, making it true for any arbitrarily large initial condition.

In addition, for $V(z(t)) \leq 1$

$$V^{1-a}(z(t)) \leq V_0^{1-a} + (1-a)(\rho_1 - \zeta_1 t)$$

Here, $0 < (1-a) < 1$, and the maximum value of $V(z(t))$ could be 1. Hence, $V^{1-a}(z(t)) \leq 1 + (1-a)(\rho_1 - \zeta_1 t)$, which guarantees that $V(z(t)) = 0$ for $t \geq \frac{\rho_1}{\zeta_1} + \frac{1}{(1-a)\zeta_1}$.

So, $V(z(t)) = 0$ for all

$$t \geq T_{max} = \frac{\rho_1}{\zeta_1} + \frac{1}{(1-a)\zeta_1} + \frac{\rho_2}{\zeta_2} + \frac{1}{(b-1)\zeta_2}$$

for any initial condition $z_0 \in \mathbb{R}^n$, where $T_{\max}$ is the maximum time of convergence. □

4. Illustrative example

In this section the efficacy of the proposed method is demonstrated by considering the following numerical example.

$$\dot{z}(t) = z(t) + u(t) - |z(t)|^{0.5}\text{sign}(z(t)) - |z(t)|^2\text{sign}(z(t)) \tag{26}$$

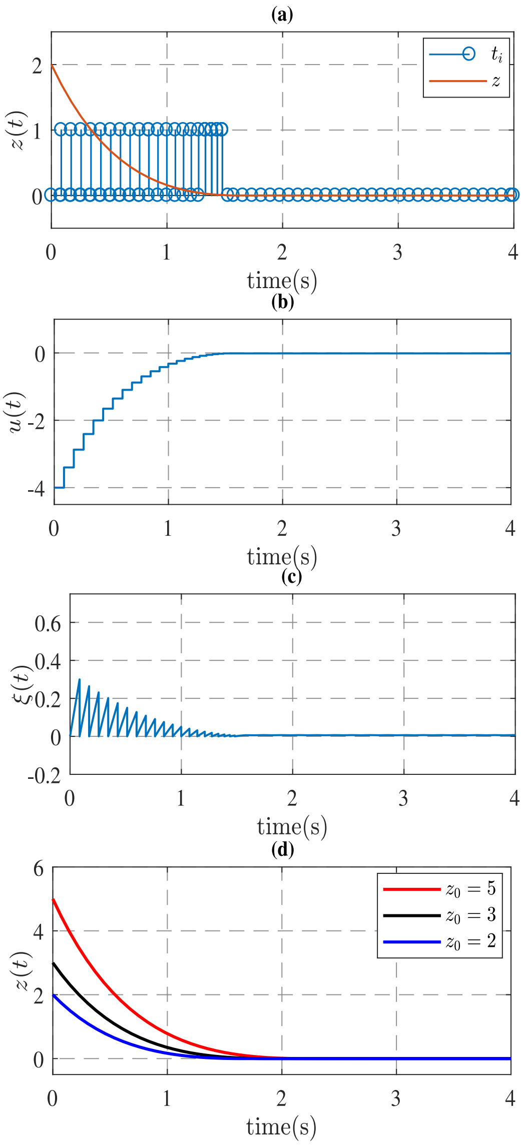

Fig. 4. Finite-time stabilization [6] without DoS attack **(a)** state evolution without DoS for $z_0 = 2$, where Blue bars are event triggering instances, **(b)** $u(t)$ without DoS, **(c)** $\xi(t)$ without DoS, **(d)** State evolution without DoS for different initial conditions (z_0).

The solution of (26) can be defined in the sense of Polyakov [18]. Now, under the control law $u(t) = \phi(z(t), \xi(t)) = -2z(t_{i(t)}) = -2z(t) - 2\xi(t)$, choosing the Lyapunov function as $V = z^2(t)$ and taking time derivative of V, we get:

$$\begin{aligned}\dot{V} =&2z(t)\dot{z}(t)\\ =&2z(t)(z(t)+u(t) - |z(t)|^{0.5}\text{sign}(z(t)) - z(t)^2\text{sign}(z(t)))\\ =&2z(t)(-z(t) - 2\xi(t) - |z(t)|^{0.5}\text{sign}(z(t)) - z(t)^2\text{sign}(z(t)))\\ =&-2z(t)^2 - 4z(t)\xi(t) - 2|z(t)|^{1.5} - 2|z(t)|^3\\ \le&-2z(t)^2 + 2z(t)^2 + 2\xi(t)^2 - 2|z(t)|^{1.5} - 2|z(t)|^3\\ =&-2V^{0.75} - 2V^{1.5} + 2\xi(t)^2\end{aligned}$$

So, we can say that the Lyapunov function of the form (8) exists which concludes that the system (26) is fixed-time ISS with the parameters $c_1 = 2$, $c_2 = 2$, $a = 0.75$, $b = 1.5$ and $\gamma(\|\xi(t)\|) = 2\xi(t)^2$. Now for simulation, taking for instance $\epsilon = 0.35$ the event-triggering condition (9) is obtained as $t_{i+1} = \inf\{t > t_i | 32\xi(t)^2 > 1.3|z(t)|^{1.5} + 1.3|z(t)|^3\}$. The obtained results are shown in Fig. 2.

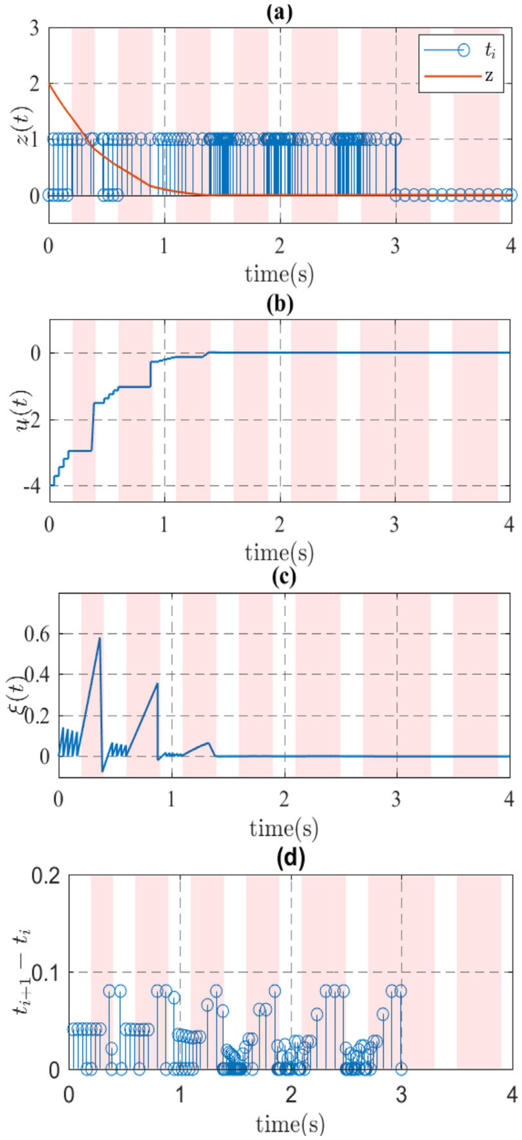

Fig. 5. Finite-time stabilization [6] with DoS attack **(a)** State evolution with DoS for $z_0 = 2$, where Blue bars are event triggering instances and vertical red stripes are time intervals of DoS, **(b)** $u(t)$ with DoS, **(c)** $\xi(t)$ with DoS, **(d)** Inter-event interval with DoS. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Additionally, under DoS attacks the performance of the designed event-triggering is proposed next. As per Definition 2 $\psi_1(\|z\|) = \frac{1}{2}z^2$ and $\psi_2(\|z\|) = 3z^2$ can be selected. Now the value of $\mu_1 = 35$ and $\mu_2 = 30$ are selected so that they satisfy Assumption 2 i.e, $32\|z\|^2 \le \mu_1\psi_1^{0.75}(\|z\|) + \psi_1^{1.5}(\|z\|)$. In order to obtain the condition on DoS frequency and time-duration $\Delta_i = \Delta_2 = 0.1$ can be chosen so that it satisfies (24), which leads to $\frac{1}{T} + \frac{0.1}{\tau_D} < 0.01129$ and $\frac{1}{T} + \frac{0.1}{\tau_D} < 0.00972$. By tuning the parameters c_1, c_2, μ_1, μ_2, ϵ the bound (24) can be changed. So by selecting appropriate values of the parameter designer can obtain the convergence as required. Here for simulation we take random DOS attacks with frequency $n(4) = 7$ and time-duration $|s(4)| \simeq 3$ in time interval of [0,4] and obtained results are shown in Fig. 3.

The proposed stabilization method is assessed and shown to be effective by comparing with the existing results on finite-time stabilization under DoS [6]. The structure and design parameters of the existing finite-time method are detailed in Reference [6]. The results are obtained considering the same DoS interval as of proposed case. Fig. 4 shows the simulation results for the existing finite-time method without the DoS attack. While Fig. 4 shows the state evolution, control input, error signal and inter-event interval of the closed-loop system under DoS attack. From the obtained results, it can be observed that although the limited time convergence is obtained with the scheme proposed in Doostmohammadian and Meskin [6], however the convergence time still depends on the initial condition of the states variable. which may results in deteriorating the entire performance of the closed-loop system. On the other-hand with the proposed control scheme one can guarantee the convergence of the state to the origin irrespective of the initial conditions, which is notorious feature of the proposed control scheme compared to existing [6].

5. Conclusion

This paper highlights the notion of fixed-time ISS for a networked control system under DoS attacks. The proof of stability is given for both the cases when there is no DoS and when there is DoS. A numerical example is simulated for the different initial conditions of the state of the system. It is shown that under what condition on DoS frequency and time duration the fixed-time ISS of the closed-loop system is well preserved by the designed control law.

For future scope directions in field of networked control with different types of DoS attacks along with disturbances and dynamic event-triggering can be considered.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] S.P. Bhat, D.S. Bernstein, Finite-time stability of continuous autonomous systems, SIAM J. Control Optim. 38 (3) (2000) 751–766.

[2] A. Cetinkaya, H. Ishii, T. Hayakawa, An overview on denial-of-service attacks in control systems: attack models and security analyses, Entropy 21 (2) (2019) 210.

[3] C. De Persis, P. Tesi, Input-to-state stabilizing control under denial-of-service, IEEE Trans. Autom. Control 60 (11) (2015) 2930–2944.

[4] C. De Persis, P. Tesi, Networked control of nonlinear systems under denial-of-service, Syst. Control Lett. 96 (2016) 124–131.

[5] V.S. Dolk, P. Tesi, C. De Persis, W.P.M.H. Heemels, Event-triggered control systems under denial-of-service attacks, IEEE Trans. Control Netw. Syst. 4 (1) (2016) 93–105.

[6] M. Doostmohammadian, N. Meskin, Finite-time stability under denial of service, IEEE Syst. J. 15 (1) (2020) 1048–1055.

[7] M. Doostmohammadian, H.R. Rabiee, U.A. Khan, Cyber-social systems: modeling, inference, and optimal design, IEEE Syst. J. 14 (1) (2019) 73–83.

[8] S. Feng, P. Tesi, Resilient control under denial-of-service: robust design, Automatica 79 (2017) 42–51.

[9] H.S. Foroush, S. Martinez, On event-triggered control of linear systems under periodic denial-of-service jamming attacks, in: 2012 IEEE 51st IEEE Conference on Decision and Control (CDC), IEEE, 2012, pp. 2551–2556.

[10] M. Golestani, S.M. Esmaeilzadeh, S. Mobayen, Fixed-time control for high–precision attitude stabilization of flexible spacecraft, Eur. J. Control 57 (2021) 222–231.

[11] Y. Hong, Z.-P. Jiang, G. Feng, Finite-time input-to-state stability and applications to finite-time control design, SIAM J. Control Optim. 48 (7) (2010) 4395–4418.

[12] K. Ji, W.-j. Kim, Stabilization of networked control system with time delays and data-packet losses, Eur. J. Control 13 (4) (2007) 343–350.

[13] S. Kanakalakshmi, R. Sakthivel, S.A. Karthick, A. Leelamani, A. Parivallal, Finite–time decentralized event-triggering non-fragile control for fuzzy neural networks with cyber-attack and energy constraints, Eur. J. Control 57 (2021) 135–146.

[14] J. Liu, Y. Zhang, Y. Yu, H. Liu, C. Sun, A Zeno-free self-triggered approach to practical fixed-time consensus tracking with input delay, IEEE Trans. Syst., Man, Cybern. 52 (5) (2021) 3126–3136.

[15] F. Lopez-Ramirez, D. Efimov, A. Polyakov, W. Perruquetti, Finite-time and fixed–time input-to-state stability: explicit and implicit approaches, Syst. Control Lett. 144 (2020) 104775.

[16] R. Merco, F. Ferrante, P. Pisu, On dos resiliency analysis of networked control systems: trade-off between jamming actions and network delays, IEEE Control Syst. Lett. 3 (3) (2019) 559–564.

[17] P.S.P. Pessim, M.J. Lacerda, State-feedback control for cyber-physical LPV systems under dos attacks, IEEE Control Syst. Lett. 5 (3) (2020) 1043–1048.

[18] A. Polyakov, Nonlinear feedback design for fixed-time stabilization of linear control systems, IEEE Trans. Autom. Control 57 (8) (2011) 2106–2110.

[19] B. Ramasubramanian, M.A. Rajan, M.G. Chandra, R. Cleaveland, S.I. Marcus, Resilience to denial-of-service and integrity attacks: a structured systems approach, Eur. J. Control 63 (2022) 61–69.

[20] V. Rezaei, M. Stefanovic, Event-triggered robust cooperative stabilization in nonlinearly interconnected multiagent systems, Eur. J. Control 48 (2019) 9–20.

[21] H. Sandberg, S. Amin, K.H. Johansson, Cyberphysical security in networked control systems: an introduction to the issue, IEEE Control Syst. Mag. 35 (1) (2015) 20–23.

[22] L. Shi, Q. Liu, J. Shao, Y. Cheng, Distributed localization in wireless sensor networks under denial-of-service attacks, IEEE Control Syst. Lett. 5 (2) (2020) 493–498.

[23] P. Tabuada, Event-triggered real-time scheduling of stabilizing control tasks, IEEE Trans. Autom. Control 52 (9) (2007) 1680–1685.

[24] Y. Xia, D.J. Hill, Attack vulnerability of complex communication networks, IEEE Trans. Circuits Syst. II 55 (1) (2008) 65–69.

[25] Y. Xia, W. Yang, Z. Zhao, Consensus-based filtering under false data injection attacks, Eur. J. Control 48 (2019) 3–8.

[26] W. Xu, K. Ma, W. Trappe, Y. Zhang, Jamming sensor networks: attack and defense strategies, IEEE Netw. 20 (3) (2006) 41–47.

[27] M. Yu, L. Wang, T. Chu, F. Hao, Stabilization of networked control systems with data packet dropout and transmission delays: continuous-time case, Eur. J. Control 11 (1) (2005) 40–49.

[28] W. Zhang, M.S. Branicky, S.M. Phillips, Stability of networked control systems, IEEE Control Syst. Mag. 21 (1) (2001) 84–99.

[29] X.-M. Zhang, Q.-L. Han, Y. Xinghuo, Survey on recent advances in networked control systems, IEEE Trans. Ind. Inform. 12 (5) (2015) 1740–1752.

[30] N. Zhao, P. Shi, W. Xing, J. Chambers, Observer-based event-triggered approach for stochastic networked control systems under denial of service attacks, IEEE Trans. Control Netw. Syst. 8 (1) (2020) 158–167.