SCIENCE CHINA
Information Sciences

• LETTER •

February 2021, Vol. 64 129203:1–129203:3
https://doi.org/10.1007/s11432-018-9583-2

Stability of networked control system subject to denial-of-service

Li GUO, Tingting CUI, Hao YU & Fei HAO*

The Seventh Research Division, School of Automation Science and Electrical Engineering, Beihang University, Beijing 100191*, China*

Received 29 June 2018/Accepted 20 August 2018/Published online 24 April 2020

Citation Guo L, Cui T T, Yu H, et al. Stability of networked control system subject to denial-of-service. Sci China Inf Sci, 2021, 64(2): 129203, https://doi.org/10.1007/s11432-018-9583-2

Dear editor,

In recent years, networked control systems (NCSs) have received ever-increasing interest from researchers owing to the advantages of improving flexibility and efficiency of systems and decreasing maintenance costs. However, the growing openness of NCSs, highly depending on network communication technology, induces many unforeseen vulnerabilities in the control systems and leads to increasing security risks as highlighted in [1]. Adversaries can easily exploit these vulnerabilities to launch attacks to degrade performance of systems, and even destroy the stability of systems in the worst case. Hence, secure control of networked control systems have been a subject of significant research interest for the last two decades (e.g., [2, 3]). Denial-of-service (DoS) attack is perhaps one of the most detrimental attacks that affect the packet delivery. By blocking the communication link and effectively preventing transmission of packets between the plant and the controller, DoS attacks could destroy the availability of signals among different nodes of the NCSs, and furthermore, drive the systems to be unstable.

Traditionally, the majority of networked control theories are based on the time-triggered manner, i.e., the sampling of the sensor and updating of the controller are executed periodically. Although periodic sampling is preferred in analysis and design, it is sometimes less preferable from a resource utilization point of view. Recently, event-triggered control (ETC) has gained more and more attention owing to the advantages of saving communication and computation resources. In ETC, control tasks are executed after the occurrence of an event, which is generated by designed triggering conditions or enent-triggered mechanism, instead of a certain fixed period of time [4–6].

A number of studies showed that event-triggered control can significantly mitigate communication traffic over the networks and retain a satisfactory closed-loop performance [4–6]. Compared with traditional time-triggered control, it may be an interesting problem whether the ETC scheme is more sensitive to networked attacks. Thus, it is necessary and important to investigate the stability of event-triggered control systems subject to DoS attacks.

Motivated by the above observations, this study focuses on the security control problem for a class of discrete-time linear time-invariant ETC systems subject to noises and DoS attacks. Also, consecutive DoS attacks are allowed. For discrete-time systems, the probability-distribution function method is a main solution in handling the phenomenon of network attacks. Thus, following [7], a random model obeying Bernoulli distribution is exploited to describe the behaviors of DoS attacks. Some sufficient conditions are developed to guarantee the input-to-state stability of systems with respect to noises. Owing to the randomness of the disturbances and attacks, the proposed method in this study is suitable for single or successive packet dropouts.

Problem formulation. Consider an NCS shown in Figure 1. The discrete-time linear time-invariant plant is described by

$$x_{k+1} = Ax_k + B_1u_k + B_2w_k, \tag{1}$$

where $x_k \in \mathbb{R}^n$ and $u_k \in \mathbb{R}^m$ are the state vector and the control input, respectively. $w_k \in \mathbb{R}^P$ is the zero mean Gaussian noises with expected value $\mathrm{E}[w_k^{\mathrm{T}} w_k] = 1$. A, B_1, B_2 are constant matrices with appropriate dimensions and (A, B_1) is controllable. Instead of using conventional periodic sampled-data control, this study considers ETC schems. As shown in Figure 1, buffer in sensor-to-controller (SC) channel (buffer SC) is employed to hold the most recently transmitted measurement of the state to the controller. From the perspective of the defenders, this can be regarded as a kind of protection mechanism. Let $\tilde{x}_k$ be the data stored in the buffer SC. Thus, in the absence of DoS attacks, the input signal can be described by

$$u_k = \begin{cases} Kx_k, & k = k_i, \\ K\tilde{x}_k, & k \neq k_i, \end{cases} \tag{2}$$

for $k \in \{k_i, k_i+1, \ldots, k_{i+1}-1\}$, $i \in N_0$, where $K \in \mathbb{R}^{m\times n}$ is the controller gain matrix such that $A+BK$ is Schur stable. Consider the following triggering condition:

$$\|\tilde{x}_k - x_k\| > \sigma\|x_k\|, \tag{3}$$

[*] Corresponding author (email: fhao@buaa.edu.cn)

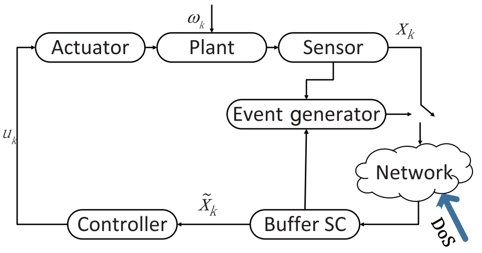

Figure 1 (Color online) DoS attacks on the closed-loop system.

where $\sigma \in \mathbb{R}_{>0}$ is a free parameter to be designed. And the sequence $\{k_i\}$ denotes the triggering time instants decided by the designed triggering condition with $k_0 = 0$ by convention. New state measurements are transmitted to the controller only when the triggering condition (3) is satisfied.

Next, consider the case with DoS attacks, which is referred to as the fail of transmission at some triggering instants. In other words, the case with DoS attacks would only occur at the triggering instants, i.e., on sequence $\{k_i\}$. Let $\alpha_{k_i} = 1$ or 0 denote whether the DoS attacks do exist or not in the channel SC. Referring to [7], assume α_{k_i} is Bernoulli varible with the following probabilities:

$$P\{\alpha_{k_i} = 1\} = \bar{\alpha}, \quad P\{\alpha_{k_i} = 0\} = 1 - \bar{\alpha}. \tag{4}$$

Clearly, Eq. (4) can yield $\mathrm{E}[\alpha_{k_i}] = \bar{\alpha}$.

In addition, in order to improve the reliability of systems, an authentication signal, denoted by D_{k_i}, is introduced. This singal is usually used to detect whether DoS attacks happen. It is measured at each triggering time instant when the triggering condition (3) is satisfied. $D_{k_i} = 0$ denotes that no attack happens at time instant k_i, while $D_{k_i} = 1$ denotes that DoS attack happens. If $D_{k_i} = 1$, the event-triggered controller would always be triggered at the next triggering time k_{i+1}. Of course, the data transmitted at the next sampling time might be attacked.

Then, the dynamics of $\tilde{x}_k$ can be described by

$$\tilde{x}_{k+1} = \begin{cases} (1-\alpha_{k_i})x_k + \alpha_{k_i}\tilde{x}_k, & k = k_i, \\ \tilde{x}_k, & k \neq k_i. \end{cases} \tag{5}$$

Under the DoS attacks of the channel SC, Eq. (2) can be rewritten as

$$u_k = \begin{cases} (1-\alpha_{k_i})Kx_k + \alpha_{k_i}K\tilde{x}_k, & k = k_i, \\ K\tilde{x}_k, & k \neq k_i. \end{cases} \tag{6}$$

Remark 1. In ETC systems, generally assume that $k_0 = 0$. However, the systems could be attacked at the process start-up. Therefore, $\alpha_{k_0} = 1$ implies that the DoS attack happens at the beginning. This raises the question of assigning a value to the buffer when communication is not possible at the initial time. Here, we assume that $\tilde{x}_0 = 0$ and $\tilde{u}_0 = 0$ if $\alpha_{k_0} = 1$.

Let $z_k = [x_k^{\mathrm{T}}, \tilde{x}_k^{\mathrm{T}}]^{\mathrm{T}}$. The ETC systems subject to DoS attacks can be obtained. It follows from (1), (5) and (6) that

$$\begin{aligned} &z_{k+1} \\ &= \begin{cases} (1-\alpha_{k_i})A_1 z_k + \alpha_{k_i} A_2 z_k + \Lambda_1 w_k, & k = k_i, \\ A_1 z_k + \Lambda_2(\tilde{x}_k - x_k) + \Lambda_1 w_k, & k \neq k_i, \end{cases} \end{aligned} \tag{7}$$

for $k \in \{k_i, k_i+1, \ldots, k_{i+1}-1\}$, $i \in N_0$, where

$$A_1 = \begin{bmatrix} A + B_1 K & 0_{n\times n} \\ I_{n\times n} & 0_{n\times n} \end{bmatrix}, \quad \Lambda_1 = \begin{bmatrix} B_2 \\ 0_{n\times m} \end{bmatrix},$$

$$A_2 = \begin{bmatrix} A & B_1 K \\ 0_{n\times n} & I_{n\times n} \end{bmatrix}, \quad \Lambda_2 = \begin{bmatrix} B_1 K \\ I_{n\times n} \end{bmatrix}.$$

The main objective of this study is to design event-triggering conditions of the form (3) such that the corresponding closed-loop system (7) is stable.

Definition 1 ([8])**.** The system (7) is said to be mean-square input-to-state stable (ms-ISS) if there exist functions $\varphi \in \mathcal{KL}$ and $\xi \in \mathcal{K}$ such that the state x_k satisfies

$$\mathrm{E}[\|x_k\|^2] \leqslant \varphi(\mathrm{E}(\|x_0\|^2), k) + \xi(\mathrm{E}[w_k^{\mathrm{T}} w_k]) \tag{8}$$

for all $k \in \mathbb{N}_0$. If (8) holds when $w_k = 0$, then the system is said to be mean-square globally asymptotically stable (ms-GAS).

Main results. Sufficient conditions to ensure stability of the closed-loop event-triggered networked control systems with DoS attacks are provided, and the concept of the largest attack probability is proposed.

Theorem 1. Assume that the attack probability $\bar{\alpha}$ in (4) is known. Then system (7) is ms-ISS if there exist a constant $\upsilon \in (0,1)$, a positive scalar κ, and symmetric positive definite matrices P and Q such that

(1) The following matrix inequality

$$\begin{bmatrix} A_1^{\mathrm{T}} P A_1 - \upsilon P & -A_1^{\mathrm{T}} P \Lambda_2 \\ * & \Lambda_2^{\mathrm{T}} P \Lambda_2 - \kappa I \end{bmatrix} < 0 \tag{9}$$

holds, and $\sigma \in (0, \sqrt{(1-\upsilon)\lambda_{\min}(P)/\kappa})$ in (3), where $\lambda_{\min}(P)$ is the minimum eigenvalue of P;

(2) P and Q are the solution of the following equation:

$$\bar{\alpha} A_2^{\mathrm{T}} P A_2 + (1-\bar{\alpha}) A_1^{\mathrm{T}} P A_1 + Q = P. \tag{10}$$

Especially, the system (7) is ms-GAS if $w_k = 0$. See Appendix A for the proof of Theorem 1.

Remark 2. Theorem 1 provides sufficient conditions to ensure the ms-ISS of the system. A method for designing the feedback controller gain matrix K could be provided based on Theorem 1, which can be found in Appendix D.

It is noted that Theorem 1 has some deficiencies. On the one hand, (9) is not a linear matrix inequality. On the other hand, the solution to (9) is obtained under the equation constraints in (10). The above deficiencies make the solving process complicated. Before presenting the correlative results, we firstly give Definition 2.

Definition 2 ([7])**.** The largest attack probability, denoted by $\alpha_{\max}$, is a positive bound such that (9) and (10) in Theorem 1 hold under any attack probability less than this bound.

Theorem 2. The largest attack probability $\alpha_{\max}$ can be obtained by the following optimization problem:

$$\begin{aligned} &\max\ \bar{\alpha} \\ &\text{s.t. } A_1^{\mathrm{T}} P A_1 - P < 0, && (11) \\ &\quad\ \bar{\alpha} A_2^{\mathrm{T}} P A_2 + (1-\bar{\alpha}) A_1^{\mathrm{T}} P A_1 - P < 0. && (12) \end{aligned}$$

In addition, for any $\bar{\alpha} \in (0, \alpha_{\max})$, (11) and (12) are always satisfied with some positive definite matrix P. See Appendix B for the proof of Theorem 2.

Remark 3. Note that constraints (11) and (12) are linear matrix inequalities for a given $\bar{\alpha}$. Thus, the sub-optimal solution with arbitrary precision can be obtained by linear search method.

Obviously, the event-triggered control is close to the time-triggered control along with a small σ. Correlative content is proposed in Appendix C.

Simulations are provided in Appendix E to illustrate the efficiency of the obtained results.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61573036, 61174057).

Supporting information Appendixes A–E. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Corona I, Giacinto G, Roli F. Adversarial attacks against intrusion detection systems: taxonomy, solutions and open issues. Inf Sci, 2013, 239: 201–225

2 Teixeira A, Shames I, Sandberg H, et al. A secure control framework for resource-limited adversaries. Automatica, 2015, 51: 135–148

3 Huda S, Miah S, Hassan M M, et al. Defending unknown attacks on cyber-physical systems by semi-supervised approach and available unlabeled data. Inf Sci, 2017, 379: 211–228

4 Tabuada P. Event-triggered real-time scheduling of stabilizing control tasks. IEEE Trans Autom Control, 2007, 52: 1680–1685

5 Wu W, Reimann S, Görges D, et al. Event-triggered control for discrete-time linear systems subject to bounded disturbance. Int J Robust Nonlinear Control, 2016, 26: 1902–1918

6 Yu H, Hao F. Input-to-state stability of integral-based event-triggered control for linear plants. Automatica, 2017, 85: 248–255

7 Hu S, Yan W Y. Stability robustness of networked control systems with respect to packet loss. Automatica, 2007, 43: 1243–1248

8 Zhu Q, Hu G D, Zeng L. Mean-square exponential input-to-state stability of euler-maruyama method applied to stochastic control systems. Acta Autom Sin, 2010, 36: 406–411