第51卷第1期 中国科学技术大学学报 Vol. 51, No. 1
2021年1月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Jan. 2021
Received: 2020-09-28; Revised: 2020-11-11 doi:10.52396/JUST-2020-1137

Multi-path switching protection for networked control systems under unbounded DoS attacks

Zhu Qiaohui[1], Liang Qipeng[1], Kang Yu[2], Zhao Yunbo[1,2*]
1. College of Information Engineering, Zhejiang University of Technology, Hangzhou 310000, China;
2. School of Information Science and Technology, University of Science and Technology of China, Hefei 230027, China
* Corresponding author. E-mail: ybzhao@ustc.edu.cn

Abstract: The strategy design and closed-loop stability of networked control systems under unbounded denial of service (DoS) attacks are probed. A multi-path switching protection strategy is firstly designed by noticing the usually available multiple paths in data communication networks. The strategy consists of a DoS attack detection module at the actuator side to identify DoS attacks from normal data packet dropouts, and a multi-path switching module at the sensor side to effectively switch the data transmission path when necessary. Then, the sufficient conditions for the closed-loop system being global mean square asymptotic stability are given, with a corresponding controller gain design method. Numerical examples illustrate the effectiveness of the proposed approach.

Keywords: networked control systems; unbounded DoS attack; DoS attack detection; multi-path switching
CLC number: O643.36 **Document code**: A

1 Introduction

Networked Control Systems (NCSs), whose data transmission channels are closed by some form of data communication networks such as the Internet, have witnessed its fast development and wide applications in recent years[1,2], due to its unique advantages including, e.g., the structural flexibility, the reduced overall cost, the easier implementation, etc[3,4]. These advantages are, however, not obtained at no cost; in fact, the unique characteristics introduced by the inserted data communication networks such as network-induced delay[5,6], data packet dropout[7-9], etc., have already been challenging control theorists and engineers in this field for decades. In recent years, besides these long-going challenges, the security issue has become one main focus[10-14], since the open and often shared data communication network in NCSs is so convenient for the attackers to intrude.

Among these network attacks, the Denial of Service (DoS) attack is the most often seen which can cause severe consequences to NCSs[15-21]. A DoS attack plays its role by sending massive requests to the target machine to exhaust all the network resources, thus failing the legitimate users. As the result of a DoS attack, the controller (actuator) in NCSs will be unable to receive data from the sensor (controller), and therefore the considered NCS will be forced to run in the open-loop, resulting in severe disasters[22-24].

In order to deal with the above challenge, considerable work has already been done, for periodic DoS attacks[25-27], random DoS attacks[28-33], on-off Dos attacks[34,35], and so forth. The considered models and approaches include queuing models[28], Bernoulli modeling[29-31] for DoS attacks, the Markov modeling of DoS attacks[32,33], the frequency and duration description of DoS attacks[35], the periodic event-triggered resilient control under DoS attacks[36], the design and analysis of multi-channel NCSs under DoS attacks[35,38], pulse control that maximizes the frequency and duration of the tolerable DoS attack[39], the design of adaptive-event-triggered filter under DoS attacks[40], just to name a few.

We observe that most existing works assume that the DoS attack is somewhat bounded, either in its frequency, or duration, or some other index. Such an assumption means that the data exchange in the NCSs is not completely shut down under DoS attacks and hence various control approaches can be proposed to stabilize the system in such a scenario. Though this bounded DoS attack assumption can be fair and sound in the community of communication networks, it may not be

Citation: Zhu Qiaohui, Liang Qipeng, Kang Yu, et al. Multi-path switching protection for networked control systems under unbounded DoS attacks. J. Univ. Sci. Tech. China, 2021, 51(1): 22-32.

appropriate for NCSs. In fact, one can readily realize that an NCS can be permanently damaged as long as the system is left open-loop for a sufficiently long time. Therefore, to DoS attack an NCS, the attacker should either be strong enough to kill the NCS at one round by forcing it open-loop for a sufficiently long time, or otherwise be too unwise to start any attack at the first instance. For such an " unbounded" DoS attack, conventional approaches will not work since the data exchange has been completely shut down.

The above observation on the " unbounded" DoS attack motivates this present work. Unlike most existing works with the frequency and duration constraints of the DoS attack, here we assume no power boundary. This assumption basically means that any control strategy relying on the constraints of the DoS attacker will not work. To deal with this challenge, we seek for help from the intrinsic nature of large data communication networks, where there are often many independent paths from the data sender to the receiver. This " multi-path" privilege then justifies our strategy: whenever the current path is attacked, the NCS should move to another path as soon as possible to recover the data transmission. Following this philosophy, in this paper we propose a so-called " multi-path switching protection" strategy, which can effectively detect the occurring DoS attack, and then switch the data transmission path to close the NCS. Under this strategy, we provide the sufficient conditions for the global mean square asymptotic stability of the closed-loop system, and numerical examples will illustrate the effectiveness of the proposed approach.

The remainder of the paper is organized as follows. Section 2 formulates the problem of interest, and section 3 discusses the attack detection method and the multi-path switching protection strategy. Then, Section 4 gives the sufficient conditions to ensure the global mean square asymptotic stability of the system under the designed multi-path switching protection strategy, and the controller is designed on this basis. The effectiveness of the proposed approach is demonstrated through numerical simulation in Section 5, and the paper is concluded in Section 4.

2 Related works and problem formulation

Consider the system setup as shown in Figure 1, where the sensing data from the sensor the controller and the control data from the controller to the actuator are transmitted via the data communication network, and the plant is modeled as a linear discrete-time system as

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

In our system setup in Figure 1, the data communication networks are assumed to have three features: ① Data transmissions are subject to unbounded DoS attacks; ② Data transmissions can be lossy in a stochastic nature; ③ For both the sensor-to-controller and the controller-to-actuator channels, multiple independent paths exist for data transmissions. These assumptions are further discussed in detail in what follows.

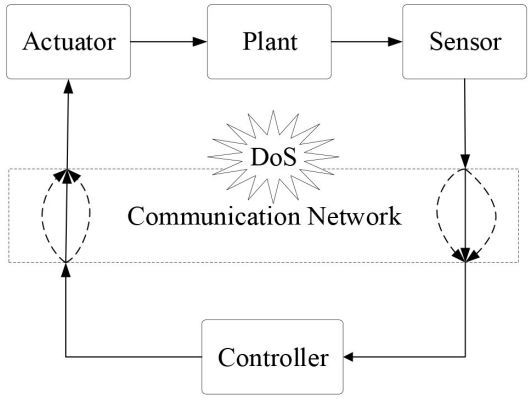

Figure 1. Illustrating networked control systems under DoS attack, where multiple independent paths exist for both the sensor-to-controller and the controller-two-actuator channels.

2.1 Unbounded DoS attacks

DoS attacks are common in data communication networks which are often exposed to the open space. In such type of attacks, the DoS attacker can simply generate massive useless data transmission requests to jam the channel. Since NCSs are essentially relying on data communication networks to transmit their sensing and control data, they are not free from such attacks, and extensive works have already been seen in recent years to deal with the resulting challenges for the system design and analysis.

One can immediately see that the core to the design and analysis of NCSs under DoS attacks is first to appropriately model DoS attacks within the NCS framework. In order to explain our DoS attack model clearly, we first discuss several classic models for comparison. We use $\mathscr{A}_t$ and $\mathscr{A}_\eta$ to represent the duration and frequency of the DoS attack, and modify the original expression of each model to fit this unified frameworks, then the reader may readily compare the similarity and difference of these models.

The periodic DoS attack model[26] In such a model, the considered NCS is attacked at every time instants nT_{period} with n being integers and $T_{\text{period}}>0$ being the attack period, and the duration of each attack is T_d, $T_d<T_{\text{period}}$, that is

$$\mathscr{A}_t: T_d \tag{2a}$$

$$\mathscr{A}_\eta: \frac{1}{T_{\text{period}}} \tag{2b}$$

With the above periodic DoS attack model, the attack is deterministic and periodic, i. e., we can readily know that during $[nT_{\text{period}}, nT_{\text{period}}+T_d])$ $\forall n$ the considered

NCS is being attacked while during $[nT_{\text{period}} + T_d, (n+1)T_{\text{period}})$, $\forall n$ it is not.

The random DoS attack model[31] This original model considers a discrete-time system. In such a model, once the attack is triggered, it will last exactly one sampling period T_{sample} (for continuous-time system the duration may be changed to some other value), and whether the considered NCS is attacked at each time instant k, is determined by a random variable $\sigma(k)$ subject to the Bernoulli distribution, that is

$$\mathscr{A}_t: T_{\text{sample}} \tag{3a}$$

$$\mathscr{A}_\eta: \sigma(k) \tag{3b}$$

With the above random DoS attack model, the DoS attack is triggered with certain probability $\Pr\{\sigma(k)\}$, but for each attack the duration is constant and fixed.

The frequency and duration limited model[34] In such a model, during the time interval (τ, t), both the attack duration $\mathscr{A}_t(\tau, t)$ and the frequency $\mathscr{A}_\eta(\tau, t)$ are upper bounded as

$$\mathscr{A}_t: \mathscr{A}_t(\tau, t) \leqslant T_1 + \frac{t-\tau}{T_2},\ T_2 > 1,\ \forall \tau,\ t \tag{4a}$$

$$\mathscr{A}_\eta: \mathscr{A}_\eta(\tau, t) \leqslant \frac{\eta_1}{t-\tau} + \frac{1}{\eta_2},\ \eta_2 \geqslant T_{\text{sample}}^{\min},\ \forall \tau,\ t \tag{4b}$$

where $T_{\text{sample}}^{\min}$ is the minimum possible sampling period. With the above frequency and duration limited model, the DoS attack can be triggered in an arbitrary way, either stochastic or deterministic, as long as its duration and frequency satisfy the upper bound in equation (4).

One may readily notice that all these above three classic DoS attack models assume some type of "boundedness" of either or both of the attack duration and frequency. These assumptions seem reasonable, since attacks are at least subject to power consumption, which is always limited. Hence attacks can never be without limit.

However, one may also notice that, to destroy any practical control system, the duration and frequency of the DoS attack (whose effect is to cut the information exchange channel), do not necessarily need to be infinite, for obviously, any practical control systems can only be left open-loop without being destabilized for a limited time. In this sense, any DoS attack should always be sufficiently "unbounded" for a considered control system, and conversely, any DoS attacker that is not sufficiently powerful enough, should not start the attack at all.

The above discussion means that a more practically meaningful assumption on DoS attacks is "unbounded" as follows, which basically fails most existing studies, and motives out present work

$$\mathscr{A}_t: \text{unbounded} \tag{5a}$$

$$\mathscr{A}_\eta: \text{unbounded} \tag{5b}$$

2.2 Lossy data transmission

Besides DoS attacks, normal data transmissions without DoS attacks can still be lossy. That is, for any data packets transmitted in the considered NCS, it can reach its destination only with certain probability. Since the data transmission in the sensor-to-controller and the controller-to-actuator channels are separate and independent, and for the control system what really matters is mainly the round-trip transmission, we may consider only the combined effects of the lossy transmission in both channels. For this reason, we simply assume that the sensing data $x(k)$ can successfully reach the actuator (after being used at the controller side) with probability p. Define

$$\theta_k = \begin{cases} 1, & \text{if } x(k) \text{ is transmitted successfully} \\ 0, & \text{otherwise} \end{cases} \tag{6}$$

then it is obvious that $\Pr\{\theta_k = 1\} = 1-p$ and $\Pr\{\theta_k = 0\} = p$.

2.3 Multiple independent paths

As mentioned earlier, both the sensor-to-controller and the controller-to-actuator channels can contain multiple feasible paths to transmit the data independently (e. g. the solid and dashed paths in Figure 1). This is true in most typical data communication networks, since in these communication networks, data links are essentially unreliable, and the redundancy in data links is a common method to improve the quality of data transmissions.

As assumed in equation (5), a DoS attacker may attack the currently activated path of both the sensor-to-controller and the controller-to-actuator channels, and when such an attack happens, it is sufficiently powerful, i. e., within reasonably finite time, the control system can not recover its data transmission from the path under attack. However, with multiple independent paths of both the sensor-to-controller and the controller-to-actuator channels, it is now possible to switch the path from the currently under attack one to another free one. We may further assume that, for a path that is newly switched to, it is not that easy to be recognized and attacked, which then consequently means that with multiple independent paths the frequency of DoS attacks is naturally bounded, that is

$$\mathscr{A}_t: \text{unbounded} \tag{7b}$$

$$\mathscr{A}_\eta: < \frac{1}{T_{\text{sample}}} \tag{7b}$$

Hence, unlike the unbounded DoS attack assumption in equation (5) which basically means that no control strategy can be designed to stabilize the system, the existence of multiple independent paths makes the attack frequency $\mathscr{A}_\eta$ bounded, thus giving us the opportunity to design appropriate control strategies to stabilize the

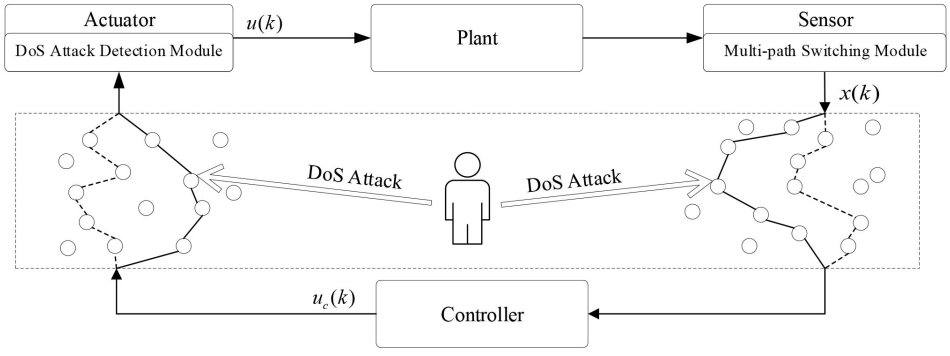

Figure 2. Illustrating the multi-path switching protection strategy for networked control systems subject to unbounded DoS attacks but with multiple independent paths.

system.

Finally, our goal in this work is to design appropriate control strategies for the system in Figure 1, where the system plant is described as in equation (1), and the data transmissions in both the sensor-to-controller and the controller-to-actuator channels are subject to both lossy transmissions as described in equation (6) and DoS attacks as in equation (7). One may realize that the co-existence of DoS attacks and lossy transmissions are the key challenge to deal with, since the existence of the normal data loss makes DoS attacks not easily identifiable, and consequently, no path switching rule can be directly implemented. In the section that follows, we will propose a DoS attack detection method, with which a path switching rule can then be defined.

3 Design of the multi-path switching protection strategy

For the NCS that suffers from unbounded DoS attacks and has multiple independent paths, we propose a multi-path switching protection strategy with two modules. The DoS attack detection module is designed in the actuator to identify whether the DoS attack is currently in progress, by comparing the difference between the random packet dropouts and the packet dropouts caused by the DoS attack. The multi-path switching module is designed on the sensor to switch paths when a DoS attack is detected. In what follows we will detail the design of the two modules and finally give the overall algorithm.

3.1 Design of the DoS attack detection module

To detect whether a DoS attack is ongoing is the first step to design the path switching rule. This however is not easy. The main challenge here is that the packet dropout itself can not be simply used as an indicator for the DoS attack, since the lossy data transmission can also cause data packet dropout.

To deal with this challenge, one may notice that packet dropouts caused by the normal lossy channel and DoS attacks should have different features. As assumed in equation (6), the former should behave probabilistically, i. e., a data packet may drop or not with certain probability, while the latter should be persistent once it occurs.

Bear this in mind, the logic to detect DoS attacks is then clear: it should be regarded as a DoS attack at time k if the recorded consecutive data packet dropouts at the actuator side, denoted by $N_d(k)$ are beyond certain threshold, denoted by N_d, or otherwise it should be regarded as normal dropouts. For example, with packet dropouts rate $p = 0.1$, the occurrence of a consecutive 5 packet loss might be regarded as a DoS attack, since the probability of causing such a consecutive 5 packet loss is as low as 0.00001 should it be only credited to random packet loss, and we have good reasons to think that an event with a low probability of 0.00001 should not easily happen in the real world.

Then, it becomes clear that for the design of the DoS attack detection module the key is first to calculate the consecutive data packet dropouts $N_d(k)$ and then determine the threshold N_d.

The determination of $N_d(k)$ can be easily done by the DoS attack detection module. We may simply run a counter within this module, which updates its value at every time instant k, either being initiated by 0 if the control signal calculated at time k, denoted by $u_c(k)$ is received, or added by 1 if otherwise. That is

$$N_d(k) = \begin{cases} 0, \text{ if } u_c(k) \text{ is received} \\ N_d(k-1) + 1, \text{ otherwise} \end{cases} \tag{8}$$

The determination of the threshold N_d can be tricky. It is readily understood that N_d being too large will mean that ongoing DoS attack is not detected while N_d being too small will mean that normal data packet dropout is detected as DoS attacks. In order to balance between these two types of errors, we introduce α reflecting the detection sensitivity and define the threshold N_d as

$$N_d = \log_p \alpha \tag{9}$$

With equations (8) and (9), the DoS attack detection module can finally be designed as

$$\sigma_d(k) = \begin{cases} \text{True, if } N_d(k) > N_d \\ \text{False, otherwise} \end{cases} \tag{10}$$

where the indicator $\sigma_d(k)$ indicates whether a DoS attack occurs at time k.

With equations (8), (9) and (10), the working logic of the DoS attack detection module can be interpreted as follows. At every time instant k, this module updates its counter $N_d(k)$ and compare it with the threshold N_d, and claims the occurrence of a DoS attack whenever $N_d(k) > N_d$. Notice that whenever the module makes such a claim, the actual consecutive data packet dropout is larger than N_d, and if conversely, no DoS attack is ongoing while these data packet dropouts are contributed by normal data loss, the probability of having larger than N_d consecutive dropouts is less than $p^{N_d} = \alpha$. Hence, α as the tunable parameter, can be used to control the balance of the aforementioned two types of errors: the larger α is, the more actual DoS attacks can be recognized, and the more normal data loss will be falsely recognized as DoS attacks. In practice, the value of α should be carefully chosen by considering both the system cost and performance.

3.2 Design of the multi-path switching module

With Subsection 3.1, the DoS attack detection module can effectively detect whether a DoS attack is ongoing. Once such an attack is detected, the current path (the solid one in Figure 2) which can not be recovered in a short time should be switched to a new available path (the dashed one in Figure 2), thanks to the multiple available paths for NCSs.

One may intuitively think that the switching rule can be simply designed as "switching the path whenever a DoS attack is detected, i.e., $\sigma_d(k)$ is *TRUE*". As the newly switched path is hardly found by the DoS attackers and hence can maintain service for some time, such a switching rule can then effectively deal with DoS attacks.

The above approach is sound should only the effects of DoS attacks be of interest. However, we notice that even without DoS attacks, the normal data loss can also produce consecutive data packet dropouts, which may destabilize the system in severe conditions. Therefore, we may take advantage of the switching module that will be designed anyway for DoS attacks to further overcome the negative effects of the normal data loss.

With the above considerations, our multi-path switching module can then be designed as

$$\sigma_P(k): \left.\begin{matrix} \text{TRUE, if } N_d(k) \geqslant N \\ \text{FALSE, otherwise} \end{matrix}\right\} \tag{11}$$

where the indicator function $\sigma_P(k)$ indicates whether the current path at time k should be switched, and the actual switching bound N is defined as

$$N = \min\{N_d, N_c\} \tag{12}$$

where N_c is the maximum number of consecutive data packet dropouts under which the considered NCS can still maintain its required performance, the determination of which will be further detailed in subsection 4.2.

With equations (11) and (12), the working logic of the multi-path switching rule can then be interpreted as follows. At every time instant k, this module obtains the current number of consecutive data packet dropouts $N_d(k)$, compares it with the actual switching bound N, and finally decides whether to switch the path according to equation (11).

3.3 The multi-path switching protection algorithm

In our system design, the controller simply generates the control signal based on its latest available sensing data and sends it to the actuator. The actuator then selects its latest available control signal to apply it to the plant. Hence, the control signal actually applied can be determined as

$$u(k) = \begin{cases} u(k-1), \text{ if under DoS attack} \\ \theta_k u_c(k) + (1-\theta_k)u(k-1), \text{ otherwise} \end{cases} \tag{13}$$

The overall algorithm of the multi-path switching protection strategy for NCSs with unbounded DoS attacks and multiple independent paths, can then be organized as in Algorithm 3.1.

Algorithmic 3.1 Multi-path switching protection algorithm

1 **Initialization** Given the plant model in equation (1), data loss probability p, and the design parameters α. Calculate the threshold N_d by equation (9), determine the allowed maximum number of consecutive data packet dropout N_c by equation (40), and calculate the actual threshold N by equation (12).

2 **Sampling** At time k, the sensor samples the plant and sends the sample $x(k)$ to the controller.

3 **Controller** The controller generates the control law and sends the control signal to the actuator.

4 **Execution and Switching Condition** The actuator applies the available control signal as in equation (13) to the plant, and its DoS attack detection module calculates the consecutive data packet dropout $N_d(k)$ by equation (8) and sends it to the sensor.

5 **Switching** The sensor decides whether to switch the path according to equation (11).

4 Stability analysis and controller design

This section first obtains the closed-loop system under the multi-path switching protection strategy proposed in Section 3, then analyzes the closed-loop system stability, and finally proposes a design method for the controller gain K.

The following concept of global mean square asymptotic stability is needed.

Definition 4.1[41] The system in equation(1) is said to be globally mean-square asymptotically stable (GMSAS), if for any given initial state $x(0)\in\mathbb{R}^n$, it holds that

$$\lim_{k\to\infty}E\{\|x(k)\|^2\}=0.$$

4.1 Closed-loop system under state feedback control

We consider a simple state feedback controller for equation(13), but we should bear in mind that any control law can be applied to equation(13) provided it can ensure the desired system performance.

For state feedback control, the general form of the control signals in equation(13) can be specified as

$$u_c(k)=Kx(k) \tag{14a}$$

$$u(k-1)=K\hat{x}(k-1) \tag{14b}$$

where the control gain K is to be designed.

Define $z(k)=[x^{\mathrm{T}}(k),\ \hat{x}^{\mathrm{T}}(k-1)]^{\mathrm{T}}$, and then the closed-loop system without DoS attack can be written as

$$z(k+1)=\Phi_{\theta_k}z(k) \tag{15}$$

where

$$\Phi_0=\begin{bmatrix}A & BK\\ 0 & I\end{bmatrix} \tag{16}$$

$$\Phi_1=\begin{bmatrix}A+BK & 0\\ I & 0\end{bmatrix} \tag{17}$$

Similarly, the closed-loop system under DoS attack can be written as

$$z(k+1)=\Phi_0z(k) \tag{18}$$

With equation(15) and (18), the closed-loop system can be written as

$$z(k+1)=\begin{cases}\Phi_{\theta_k}z(k), & t_i<k<t_{i+1}^a\\ \Phi_0z(k), & t_i^a<k<t_i\end{cases} \tag{19}$$

where t_i and t_i^a are the time of the ith switch and the ith DoS attack respectively.

4.2 Closed-loop stability

Theorem 4.1 Given ξ, p, $0<\gamma<1$, $\beta>1$, the closed-loop system in equation(19) is GMSAS, if

$$N<\frac{1/\xi+\log_\gamma c_1c_2}{1-\log_\gamma\beta} \tag{20a}$$

where $\xi=\sup\mathscr{A}_\eta$ is the upper bound of the attack frequency,

$$c_1=\frac{\lambda_{\max}\{P_0,P_1\}}{\lambda_{\min}\{P_0,P_1\}} \tag{20b}$$

$$c_2=\frac{\lambda_{\max}(P_2)}{\lambda_{\min}(P_2)} \tag{20c}$$

and P_0, P_1, P_2 are symmetric positive definite matrices that satisfy the following inequalities,

$$p\Phi_0^{\mathrm{T}}P_0\Phi_0+(1-p)\Phi_0^{\mathrm{T}}P_1\Phi_0-\gamma P_0<0 \tag{20d}$$

$$p\Phi_1^{\mathrm{T}}P_0\Phi_1+(1-p)\Phi_1^{\mathrm{T}}P_1\Phi_1-\gamma P_1<0 \tag{20e}$$

$$\Phi_0^{\mathrm{T}}P_2\Phi_0-\beta P_2<0 \tag{20f}$$

Proof We consider two subsystems, being DoS attacked or not, denoted by Σ_1 and Σ_2, respectively.

Consider subsystem Σ_1. Choose the following Lyapunov function candidate

$$V_1(k)=z^{\mathrm{T}}(k)P_{\theta_k}z(k) \tag{21}$$

Along the trajectory of the closed-loop system in equation(19), we obtain that

$$\begin{aligned}&E(V_1(k+1)\mid z(k),\theta_k)-\gamma V_1(k)=\\ &E(z^{\mathrm{T}}(k+1)P_{\theta(k+1)}z(k+1)\mid z(k),\theta_k)-\\ &\gamma z^{\mathrm{T}}(k)P_{\theta_k}z(k)=\\ &pz^{\mathrm{T}}(k)\Phi_{\theta_k}^{\mathrm{T}}P_0\Phi_{\theta_k}z(k)+\\ &(1-p)z^{\mathrm{T}}(k)\Phi_{\theta_k}^{\mathrm{T}}P_1\Phi_{\theta_k}z(k)-\gamma z^{\mathrm{T}}(k)P_{\theta_k}z(k)=\\ &z^{\mathrm{T}}(k)(p\Phi_{\theta_k}^{\mathrm{T}}P_0\Phi_{\theta_k}+(1-p)\Phi_{\theta_k}^{\mathrm{T}}P_1\Phi_{\theta_k}-\gamma P_{\theta_k})z(k)\end{aligned} \tag{22}$$

Combining equations (20d) and (20e), from equation(22) we obtain

$$E(V_1(k+1)\mid z(k),\theta_k)-\gamma V_1(k)<0 \tag{23}$$

Therefore, recursion can be obtained in subsystem Σ_1, as

$$E(V_1(k)\mid z(t_i),\theta(t_i))<\gamma^{k-t_i}V_1(t_i) \tag{24}$$

where t_i is the moment when the path is switched for the ith time, and $t_0=0$.

For any k in the subsystem Σ_1, it holds that

$$E\{\|z(k)\|^2\}<c_1\gamma^{k-t_i}E\{\|z(t_i)\|^2\} \tag{25}$$

Now consider subsystem Σ_2. Choose the following Lyapunov function candidate

$$V_2(k)=z^{\mathrm{T}}(k)P_2z(k) \tag{26}$$

Along the closed-loop system in equation(19), we obtain

$$\begin{aligned}&E(V_2(k+1)\mid z(k))-\beta V_2(k)=\\ &z^{\mathrm{T}}(k)\Phi_0^{\mathrm{T}}P_2\Phi_0z(k)-\beta z^{\mathrm{T}}(k)P_2z(k)=\\ &z^{\mathrm{T}}(k)(\Phi_0^{\mathrm{T}}P_2\Phi_0-\beta P_2)z(k)\end{aligned} \tag{27}$$

Combining (20f), from (27) we obtain

$$E(V_2(k+1)\mid z(k))-\beta V_2(k)<0 \tag{28}$$

Therefore, recursion can be obtained in subsystem Σ_2, as

$$E(V_2(k)\mid z(t_i^a))<\beta^{k-t_i^a}V_2(t_i^a) \tag{29}$$

where t_i^a is the moment of the system was attacked for the ith time.

For any k in the subsystem Σ_2, it holds that

$$E\{\|z(k)\|^2\}<c_2\beta^{k-t_i^a}E\{\|z(t_i^a)\|^2\} \tag{30}$$

In what follows we prove that

$$\|z(t_{i+1})\|<\|z(t_i)\| \tag{31}$$

In fact, by combining equations(20a), (25), (30), one obtains that

$$\begin{aligned}&E\{\|z(t_{i+1})\|^2\}<\\ &c_2\beta^{t_{i+1}-t_{i+1}^a}E\{\|z(t_{i+1}^a)\|^2\}\leqslant\\ &c_2\beta^N\{\|z(t_{i+1}^a)\|^2\}<\\ &c_2\beta^Nc_1\gamma^{t_{i+1}^a-t_i}E\{\|z(t_i)\|^2\}\leqslant\\ &c_2\beta^Nc_1\gamma^{T-N}E\{\|z(t_i)\|^2\}<\\ &[c_2\beta^Nc_1\gamma^{T-N}]^{i+1}\|z(t_0)\|^2\end{aligned} \tag{32}$$

where T is the lower bound of the interval between two adjacent attacks, $\xi = \frac{1}{T}$ represents the upper bound of the attack frequency.

With equation(32), we can rewrite equation(25) as

$$E\{\|z(k)\|^2\} < c_1\gamma^{k-t_i}E\{\|z(t_i)\|^2\} < c_1\gamma^{k-t_i}[c_2\beta^N c_1\gamma^{T-N}]^i\|z(t_0)\|^2 \quad (33)$$

Using equation(20), it yields that

$$c_2\beta^N c_1\gamma^{T-N} < 1 \quad (34)$$

Thus,

$$\lim_{i\to\infty} c_1\gamma^{k-t_i}[c_2\beta^N c_1\gamma^{T-N}]^i\|z(t_0)\|^2 = 0 \quad (35)$$

Since $E\{\|z(k)\|^2\}>0$, by combining equations (33), (35), one obtains that

$$\lim_{k\to\infty} E\{\|z(k)\|^2\} = 0 \quad (36)$$

Analogously, with equation(32), we can rewrite equation(30) as

$$E\{\|z(k)\|^2\} < c_2\beta^{k-t_i^a}E\{\|z(t_i^a)\|^2\} < c_2\beta^{k-t_i^a}c_1\gamma^{t_i^a-t_{i-1}}E\{\|z(t_{i-1})\|^2\} < c_2\beta^{k-t_i^a}c_1\gamma^{t_i^a-t_{i-1}}(c_2\beta^N c_1\gamma^{T-N})^{i-1}\|z(t_0)\|^2 \leqslant [c_2\beta^N c_1\gamma^{T-N}]^i\|z(t_0)\|^2 \quad (37)$$

Due to equation(34), it yields that

$$\lim_{i\to\infty}[c_2\beta^N c_1\gamma^{T-N}]^i\|z(t_0)\|^2 = 0 \quad (38)$$

Since $E\{\|z(k)\|^2\}>0$, by combining equations (37), (38), one obtains that

$$\lim_{k\to\infty} E\{\|z(k)\|^2\} = 0 \quad (39)$$

Finally by Definition 4.1, the closed-loop system in equation(19) is GMSAS.

From Theorem 4.1, we may determine N_c as follows to ensure the system stability,

$$N_c = \frac{1/\xi + \log_\gamma c_1 c_2}{1 - \log_\gamma \beta} \quad (40)$$

Remark 4.1 One may notice that earlier works[34,35] often assume the constraints on both the DoS attack frequency and duration to ensure the system performance, while in our present work, only attack frequency $\mathscr{A}_\eta$ is constrained. What is more, unlike these earlier works where these constraints are arbitrarily assumed, our constraint on the attack frequency makes sense in practice. Indeed, the attack frequency relies on the path switch and it is reasonable to say that for a newly switched path the attacker must take some time to find it to initiate the attack.

Additionally, according to equations (7) and (34), it can be further obtained that the GMSAS of the system can be ensured as long as the DoS attack frequency is upper bounded as

$$\mathscr{A}_\eta: < \frac{1}{N - \log_\gamma c_1 c_2 \beta^N} \quad (41)$$

4.3 Controller design

Based on Theorem 4.1, we give the following feedback gain design method.

Theorem 4.2 Given ξ, p, $0<\gamma<1$, $\beta>1$. If (20a) can be ensured with c_1, c_2 being defined in Theorem 4.1, and P_0, P_1, P_2 being the solution of the following inequalities.

$$\begin{bmatrix} -\gamma P_0 & \sqrt{p}\Phi_0^{\mathrm{T}} & \sqrt{1-p}\Phi_0^{\mathrm{T}} \\ \sqrt{p}\Phi_0 & -P_0^{-1} & \\ \sqrt{1-p}\Phi_0 & & -P_1^{-1} \end{bmatrix} < 0 \quad (42)$$

$$\begin{bmatrix} -\gamma P_1 & \sqrt{p}\Phi_1^{\mathrm{T}} & \sqrt{1-p}\Phi_1^{\mathrm{T}} \\ \sqrt{p}\Phi_1 & -P_0^{-1} & \\ \sqrt{1-p}\Phi_1 & & -P_1^{-1} \end{bmatrix} < 0 \quad (43)$$

$$\begin{bmatrix} -\beta P_2 & \Phi_0^{\mathrm{T}} \\ \Phi_0 & -P_2^{-1} \end{bmatrix} < 0 \quad (44)$$

then the control gain K as solved in equations (42), (43) and (44) ensures the GMSAS of the closed loop system in equation(19).

Proof Using Shure's complement lemma, equations (20d), (20e), (20f) can be transformed into equations (42), (43), (44), and thence the theorem can be readily obtained.

Equations (42), (43), (44) are nonlinear matrix inequalities, which cannot be solved directly using the LMI toolbox. Cone Complementary Linearization Iteration (CCL) algorithm[42] can be used to obtain an approximated solution by converting it into its linear counterpart.

5 Numerical example

Consider the system in equation (1) with an added disturbance term $w(k)$, as follows

$$x(k+1) = Ax(k) + Bu(k) + w(k).$$

In the simulation, $w(k)$ is assumed to be Gauss white noise with its variance being 0.01, and the system matrices are taken from reference [43], as

$$A = \begin{pmatrix} 0.6065 & 0 & -0.2258 \\ 0.3445 & 0.7788 & -0.0536 \\ 0 & 0 & 1.2840 \end{pmatrix},$$

$$B = \begin{pmatrix} -0.0583 \\ -0.0093 \\ 0.5681 \end{pmatrix},$$

which can be readily seen to be open-loop unstable, with their eigenvalues being 0.7788, 0.6065 and 1.2840, respectively.

In the simulation, the initial state of the considered system is set as $x(0)=[1\ 1\ 1]^{\mathrm{T}}$, and the normal data loss probability is $p=0.3$. We simulate the system for 200 time steps, and the unbounded DoS attacks occur arbitrarily, attacking the current path in use, with the upper bound of the attack frequency $\xi=0.02$.

From Theorem 4.2 and equation (40), we may obtain $N_c=13.8460$, and $N_d=9.5624$ can be determined

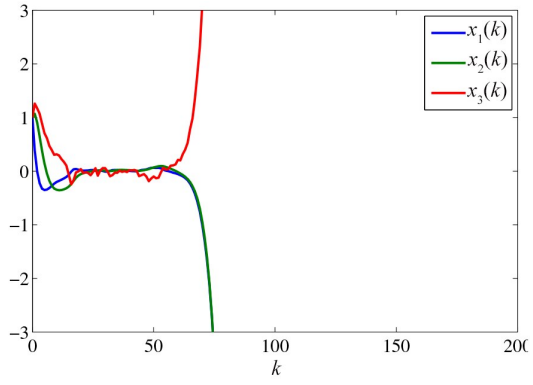

Figure 3. The considered system is unstable under unbounded DoS attack, if the proposed multi-path switching protection strategy is not in use.

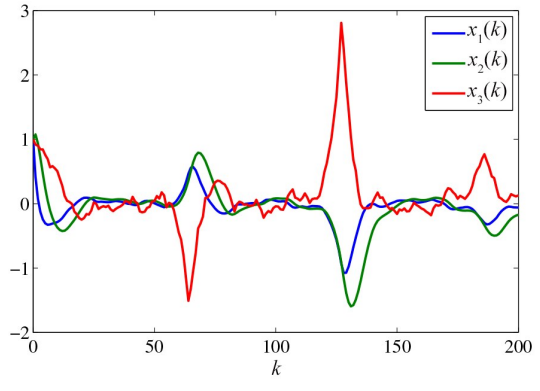

Figure 4. The considered system is stable under the unbounded DoS attack, if the proposed multi-path switching protection strategy is in use.

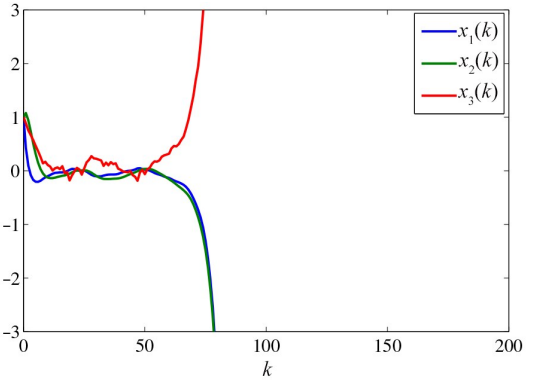

Figure 5. The state trajectory under the packet-based state feedback controller under the unbounded DoS[21].

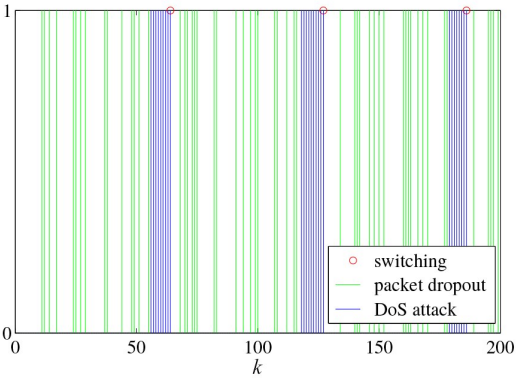

Figure 6. The multi-path switching protection strategy can effectively identify unbounded DoS attacks, and does not mistake them for normal data packet dropouts.

for $\alpha=10^{-5}$. Hence $N=N_d$. Further, using Theorem 4.2, the controller gain K can be calculated as follows (with $\gamma=0.8$, $\beta=1.1$)

$$K = [0.1490, 0.0334, -0.7513].$$

Figures 3 and 4 show the system state trajectories of two cases, either without or with the use of the proposed multi-path switching protection strategy, where DoS attacks occur at time instants 56, 118, and 179, respectively. It is readily seen from Figure 3 that without the use of our proposed strategy, the system states will become unbounded soon after the first DoS attack at time instant 56, which is understandable since the occurrence of the DoS attack means the system has to run in the open-loop afterwards. However, with the use of our proposed strategy, we see from Figure 4 that the system trajectory can soon recover from the instability trend caused by the consecutive data packet dropout due to the DoS attack, since the path switching strategy can close the control loop after a finite number of consecutive data packet dropouts.

In order to further prove the effectiveness of our proposed multi-path switching protection strategy, we compare our strategy with the packet-based state feedback controller under DoS attacks as proposed in reference [21]. Under the above system parameters, Figure 5 shows that the method in reference [21] actually destabilizes the system.

In Figure 6 we further show the time instants of normal data packet dropout (the vertical green lines), the dropouts caused by DoS attacks (the vertical blue lines), and the time instant of path switching (the red circle), under the use of the multi-path switching protection strategy. From Figure 6 we see that our multi-path switching protection strategy can effectively identify unbounded DoS attacks and seldom mistake DoS attacks from normal data packet dropouts.

In order to further evaluate the effects of α, we let $\alpha=5\times10^{-4}$ and rerun the simulation. In this case, $N_d=6.3132$, and $N=N_d$. The controller gain K remains unchanged. The system trajectories are shown in Figure 7, and the time instants of normal data packet dropouts, the unbounded DoS attacks (54, 113, and 175 respectively) and the path switching are shown in Figure 8.

By comparing Figure 4 with Figure 7, it can be

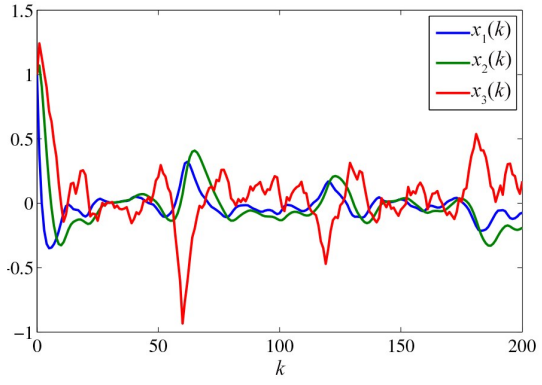

Figure 7. The considered system is stable for $\alpha=5\times10^{-4}$.

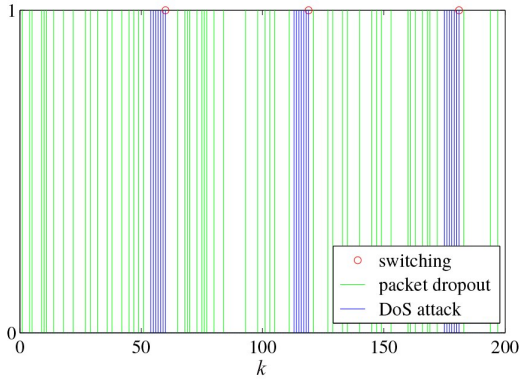

Figure 8. DoS attack, packet dropout and path switching signal when $N=6.3132$.

seen, without surprise, that the larger α is, the smaller N_c is, the faster DoS attack is identified, and finally the better the system performance can be. On the other hand, it is also not surprising to see that a larger α can mean more normal data packet dropouts being mistakenly identified as DoS attacks. In fact, from the 100 repeated experiments for both cases ($\alpha=10^{-5}$ and $\alpha=5\times10^{-4}$ respectively), we find that the false identification ratio (the number of all mistakenly identified switching divided by the total number of path switching in the 100 experiments) increases from 0.33% to 1.58%, but both are relatively small and acceptable.

6 Conclusion

Different from most existing works where the DoS attacks are usually assumed to be bounded in some sense, in the present work we claim that unbounded DoS attacks may be more often seen for networked control systems. Based on this observation, we formulate the corresponding problem, with a novel control strategy specially designed for unbounded DoS attacks, as well as the closed-loop stability analysis and numerical verifications. We believe that our work can be practically meaningful, and will further improve the design in the face of various complicated scenarios.

Acknowledgements

This work is supported by the National Key Research and Development Program of China (2018AAA0100801) and the National Natural Science Foundation of China under Grant(61673350).

Conflict of interest

The authors declare no conflict of interest.

Author information

Zhu Qiaohui received the BE degree from Tianjin University of Technology and Education, Tianjin, China, in 2018, and is currently a Postgraduate with Zhejiang University of Technology, Hangzhou, China. Her research interests include networked control systems and network security.

Ling Qipeng received his BE degree from Xi´an University of Technology, China, in 2016. He is currently pursuing a M. S. degree at College of Information Engineering, Zhejiang University of Technology. His main research interests include wireless network control systems.

Kang Yu received the PhD degree in control theory and control engineering from the University of Science and Technology of China, Hefei, China, in 2005. From 2005 to 2007, he was a Postdoctoral Fellow with the Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China. He is currently a Professor with the State Key Laboratory of Fire Science, Department of Automation, and Institute of Advanced Technology, University of Science and Technology of China, and with the Key Laboratory of Technology in GeoSpatial Information Processing and Application System, Chinese Academy of Sciences. His current research interests include monitoring of vehicle emissions, adaptive/robust control, variable structure control, mobile manipulator, and Markovian jump systems.

Zhao Yunbo received his BSc degree in mathematics from Shandong University, Jinan, China in 2003, MSc degree in systems sciences from the Key Laboratory of Systems and Control, Chinese Academy of Sciences, Beijing, China in 2007, and PhD degree in control engineering from the University of South Wales (formerly University of Glamorgan), Pontypridd, UK in 2008, respectively. He is currently a Professor with Zhejiang University of Technology, Hangzhou, China. He has worked on networked control systems for many

years and proposed a unified control framework called " packet-based control". He has also been interested in the understanding of protein synthesis by mathematically modelling such systems and discovering the underlying organization principles. His current interests mainly focus on AI-driven control and automation, specifically, AI-driven networked intelligent control, AI-driven human-machine autonomies and AI-driven machine gaming.

References

[1] Park P, Ergen S C, Fischione C, et al. Wireless network design for control systems: A survey. IEEE Communications Surveys & Tutorials, 2017, 20(2): 978-1013.

[2] Zhang D, Shi P, Wang Q G, et al. Analysis and synthesis of networked control systems: A survey of recent advances and challenges. ISA Transactions, 2017, 66: 376-392.

[3] Zhang X M, Han Q L, Yu X. Survey on recent advances in networked control systems. IEEE Transactions on Industrial Informatics, 2015, 12(5): 1740-1752.

[4] Ge X, Yang F, Han Q L. Distributed networked control systems: A brief overview. Information Sciences, 2017, 380: 117-131.

[5] Rouamel M, Gherbi S, Bourahala F. Robust stability and stabilization of networked control systems with stochastic time-varying network induced delays. Transactions of the Institute of Measurement and Control, 2020, 42(10): 1782-1796.

[6] Li Y, Liu G P, Sun S, et al. Prediction-based approach to finite-time stabilization of networked control systems with time delays and data packet dropouts. Neurocomputing, 2019, 329: 320-328.

[7] Zhang Z, Zheng W, Xie P, et al. H-infinity stability analysis and output feedback control for fuzzy stochastic networked control systems with time-varying communication delays and multipath packet dropouts. Neural Computing and Applications, 2020: 1-19.

[8] Zhao Y B, He J T, Zhu Q H, et al. Classification-based control for wireless networked control systems with lossy multipacket transmission. IEEJ Transactions on Electrical and Electronic Engineering, 2019, 14(11): 1667-1672.

[9] Zhao Y B, Huang T, Kang Y, et al. Stochastic stabilization of wireless networked control systems with lossy multi-packet transmission. IET Control Theory & Applications, 2018, 13(4): 594-601.

[10] Ding D, Han Q L, Xiang Y, et al. A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing, 2018, 275: 1674-1683.

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

[12] Li M, Chen Y. Challenging research for networked control systems: A survey. Transactions of the Institute of Measurement and Control, 2019, 41(9): 2400-2418.

[13] Mahmoud M S, Hamdan M M, Baroudi U A. Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges. Neurocomputing, 2019, 338: 101-115.

[14] Sandberg H, Amin S, Johansson K H. Cyberphysical security in networked control systems: An introduction to the issue. IEEE Control Systems Magazine, 2015, 35(1): 20-23.

[15] Shen Y, Zhang W, Ni H, et al. Guaranteed cost control of networked control systems with DoS attack and time-varying delay. International Journal of Control, Automation and Systems, 2019, 17(4): 811-821.

[16] Ten C W, Liu C C, Manimaran G. Vulnerability assessment of cybersecurity for SCADA systems. IEEE Transactions on Power Systems, 2008, 23(4): 1836-1846.

[17] Befekadu G K, Gupta V, Antsaklis P J. Risk-sensitive control under Markov modulated denial-of-service (DoS) attack strategies. IEEE Transactions on Automatic Control, 2015, 60(12): 3299-3304.

[18] Zargar S T, Joshi J, Tipper D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Communications Surveys & Tutorials, 2013, 15(4): 2046-2069.

[19] Loukas G, Öke G. Protection against denial of service attacks: A survey. The Computer Journal, 2010, 53(7): 1020-1037.

[20] Wood A D, Stankovic J A. Denial of service in sensor networks. computer, 2002, 35(10): 54-62.

[21] Lai S, Chen B, Li T, et al. Packet-based state feedback control under DoS attacks in cyber-physical systems. IEEE Transactions on Circuits and Systems II: Express Briefs, 2018, 66(8): 1421-1425.

[22] Lu A Y, Yang G H. Stability analysis for cyber-physical systems under denial-of-service attacks. IEEE Transactions on Cybernetics(Access), 2020: 1-10.

[23] Liu Y. Secure control of networked switched systems with random DoS attacks via event-triggered approach. International Journal of Control, Automation and Systems, 2020,18(5): 1-8.

[24] Yang C, Yang W, Shi H. DoS attack in centralised sensor network against state estimation. IET Control Theory & Applications, 2018, 12(9): 1244-1253.

[25] Zhu Y, Zheng W X. Observer-based control for cyber-physical systems with periodic DoS attacks via a cyclic switching strategy. IEEE Transactions on Automatic Control, 2019,65(8): 3714-3721.

[26] Hu S, Yue D, Xie X, et al. Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks. IEEE Transactions on Cybernetics, 2018, 49(12): 4271-4281.

[27] Tian E, Wang X, Peng C. Probabilistic-constrained distributed filtering for a class of nonlinear stochastic systems subject to periodic DoS attacks. IEEE Transactions on Circuits and Systems I, 2020, 67(12):5369-5379.

[28] Yue M, Wu Z, Wang J. Detecting LDoS attack bursts based on queue distribution. IET Information Security, 2019, 13(3): 285-292.

[29] Guo L, Yu H, Hao F. Event-triggered control for stochastic networked control systems against denial-of-Service attacks. Information Sciences, 2020, 527:51-69.

[30] Zhao H, Niu Y, Zhao J. Event-triggered sliding mode control of uncertain switched systems under denial-of-service attacks. Journal of the Franklin Institute, 2019, 356(18): 11414-11433.

[31] Su L, Ye D. A cooperative detection and compensation mechanism against denial-of-service attack for cyber-physical systems. Information Sciences, 2018, 444: 122-

134.
[32] Lalropuia K C, Gupta V. Modeling cyber-physical attacks based on stochastic game and Markov processes. Reliability Engineering & System Safety, 2019, 181: 28-37.
[33] Ni H, Xu Z, Cheng J, et al. Robust stochastic sampled-data-based output consensus of heterogeneous multi-agent systems subject to random DoS attack: A Markovian jumping system approach. International Journal of Control, Automation and Systems, 2019, 17(7): 1687-1698.
[34] Sun Y C, Yang G H. Event-triggered resilient control for cyber-physical systems under asynchronous DoS attacks. Information Sciences, 2018, 465: 340-352.
[35] Yuan H, Xia Y, Yang H. Resilient state estimation of cyber-physical system with multichannel transmission under DoS attack. IEEE Transactions on Systems, Man, and Cybernetics: Systems(Access), 2020: 1-12.
[36] Sun Y C, Yang G H. Periodic event-triggered resilient control for cyber-physical systems under denial-of-service attacks. Journal of the Franklin Institute, 2018, 355(13): 5613-5631.
[37] Lu A Y, Yang G H. Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service. IEEE Transactions on Automatic Control, 2017, 63(6): 1813-1820.
[38] Feng S, Tesi P. Resilient control under denial-of-service: Robust design. Automatica, 2017, 79: 42-51.
[39] Liu J, Wang Y, Cao J, et al. Secure adaptive-event-triggered filter design with input constraint and hybrid cyber attack. IEEE Transactions on Cybernetics, 2020: 1-11.
[40] Gao H, Meng X, Chen T. Stabilization of networked control systems with a new delay characterization. IEEE Transactions on Automatic Control, 2008, 53(9): 2142-2148.
[41] Li Y, Liu Y. Stability of solutions of sinular systems with delay. Control Theory and Applications, 1998,15(4): 542-550.
[42] El Ghaoui L, Oustry F, AitRami M. A cone complementarity linearization algorithm for static output-feedback and related problems. IEEE Transactions on Automatic Control, 1997, 42(8): 1171-1176.
[43] Xiong J, Lam J. Stabilization of linear systems over networks with bounded packet loss. Automatica, 2007, 43(1): 80-87.

无界 DoS 攻击下网络控制系统的多路径切换保护

朱巧慧[1],梁启鹏[1],康宇[2],赵云波[1,2*]
1. 浙江工业大学信息工程学院,浙江杭州 310026;
2. 中国科学技术大学自动化系,安徽合肥 230027

摘要: 研究了网络化控制系统在无界拒绝服务攻击下的策略设计和闭环稳定性. 首先考虑到数据通信网络中通常存在多条路径,设计了一种多路径切换保护策略. 该策略由执行器端 DoS 攻击检测模块和传感器端多路径切换模块组成,执行器端 DoS 攻击检测模块从正常的数据包丢失中识别 DoS 攻击,传感器端多路径切换模块在必要时有效切换数据传输路径. 然后,给出了闭环系统全局均方渐近稳定的充分条件,并给出了相应的控制器增益设计方法. 数值算例验证了所提方法的有效性.

关键词: 网络化控制系统;无界 DoS 攻击;DoS 攻击检测;多路径切换