ICIC Express Letters
Volume **16**, Number **8**, August **2022**
 ISSN 1881-803X
pp. **851–858**

SAMPLED-DATA CONTROL FOR NONLINEAR NETWORKED CONTROL SYSTEMS UNDER DENIAL-OF-SERVICE ATTACKS

Ning Zhao[1], Peng Shi[2,4], Wen Xing[1,*] and Huiyan Zhang[3]

[1]College of Intelligent Systems Science and Engineering
Harbin Engineering University
No. 145, Nantong Street, Nangang District, Harbin 150001, P. R. China
zhaoning@hrbeu.edu.cn; *Corresponding author: xingwen@hrbeu.edu.cn

[2]School of Electrical and Electronic Engineering
The University of Adelaide
Adelaide, SA 5005, Australia
peng.shi@adelaide.edu.au

[3]National Research Base of Intelligent Manufacturing Service
Chongqing Technology and Business University
No. 19, Xuefu Street, Nan'an District, Chongqing 400067, P. R. China
huiyanzhang@ctbu.edu.cn

[4]College of Engineering and Science
Victoria University
Melbourne, VIC, Australia
peng.shi@vu.edu.au

Received December 2021; accepted February 2022

Abstract. *This paper deals with the output feedback sampled-data control problem for networked systems described by nonstrict-feedback nonlinear systems under aperiodic denial-of-service (DoS) attacks. First, a novel switched observer is developed in the presence of DoS attacks. Second, a new switched system model is established by considering the effect of the periodic sampling and DoS attacks simultaneously. By virtue of this new model combined with a piecewise Lyapunov-Krasovskii functional method, the sufficient conditions are derived to guarantee exponential stability of the resulting switched system. Third, criteria for designing a desired observer-based sampled-data controller are provided and expressed in terms of a set of linear matrix inequalities. Finally, an illustrative example is presented to verify the efficiency of the developed control method.*
Keywords: Networked nonstrict-feedback nonlinear system, Denial-of-service attacks, Sampled-data control

1. **Introduction.** In recent years, the security control issues of networked control systems (NCSs) have received extensive attention [1, 2, 3, 4, 5]. The communication network between physical devices is vulnerable to deliberate attack, which makes the system intermittently in an open loop state and then causes the system to be paralyzed. Moreover, some attackers have caused serious accidents to networked systems, such as oil pipeline explosions and power system failures [6]. In particular, denial-of-service (DoS) attacks, which send a large amount of data to network communication channels, slow down the network response and block signal transmission, and ultimately lead to the paralysis of the communication network, posing a great security risk to NCSs [7]. Therefore, considering the impact of network attacks, it is of great practical significance to study the security control issues of NCSs.

Compared with other types of attacks, such as deception attacks and replay attacks, the DoS attacks are easy to initiate through hackers [8]. How to design defense strategies

DOI: 10.24507/icicel.16.08.851

to resist the impact of DoS attacks has attracted extensive attention and has achieved some fruitful results [9, 10, 11, 12]. A sampled-data control scheme was developed in [9] to preserve the NCS to be stable under DoS attacks which are constrained by frequency and duration in [9]. The work in [10] generalized the results in [9] to multiple transmission channels under DoS attacks, and used linear matrix inequality techniques to analyze system stability. Considering the impact of DoS attacks and constrains on network resources, the resilient event-triggered control problem for stochastic NCSs was investigated in [11]. The exponential stabilization and L_2-gain analysis problems of uncertain NCSs with aperiodic DoS attacks, time delays and external interferences were reported by using a resilient dynamic event-triggered control strategy [12].

With the rapid development of wireless digital communication, the control input commands of the practical system usually adopt a sampled-data control approach. In particular, the control signals of NCSs are generally transmitted through network media. The signal transmitted by the sensor and/or the controller through the network is only a discrete digital signal, i.e., a sampled-data signal. This control method has been widely discussed in the existing results [13, 14, 15, 16]. The discretized output feedback controller was designed to globally stabilize system by tuning the scaling gain and the maximum allowable sampling period [13]. The finite-time fuzzy switching control problem for the flexible spacecraft under stochastic failures and aperiodic sampling was presented in [14]. A nonlinear sampled-data extended state observer-based active disturbance rejection control with consideration of the actuator saturation effect was investigated for a pneumatic muscle actuator system [15]. A decentralized output feedback sampled-data control strategy was proposed to stabilize nonstrict-feedback large-scale nonlinear systems under DoS attacks via a Lyapunov approach [16].

Although the problem of sampled-data control of nonlinear systems under DoS attacks has been presented in [16], the existing methods introduce a large number of mathematical derivations and constraints. This motivates us to find a novel and simple method to solve this problem. The following are the main contributions of this article.

- A new switched system approach is presented, by which the nonlinear NCS, DoS attacks, and sampled-data control strategy are integrated into a unified framework. By using a piecewise Lyapunov-Krasovskii functional method, some new stability criteria are derived to guarantee the resulting switched system is exponentially stable.
- A solution for jointly designing the observer gain, and the control gain is provided.

The rest of the paper is arranged as follows. In Section 2, the system model, the observer and the control objective are formulated. In Section 3, main results of stability analysis and the controller and observer design are derived. Section 4 shows a simulation study for verification. Finally, the conclusion is given in Section 5.

Notation: Let $\mathbb{R}^{n\times m}$ be the sets of all $n \times m$ real matrices. The notion $\mathcal{T} > 0$ ($\mathcal{T} \geq 0$) means the matrix $\mathcal{T}$ is real symmetric and positive definite (semidefinite). The sign $\mathrm{He}(\mathcal{T})$ denotes $\mathcal{T} + \mathcal{T}^T$. The symbol $*$ represents a symmetric term induced by symmetric block matrix. diag$\{\ldots\}$ stands for a block-diagonal.

2. **Problem Statement and Preliminaries.**

2.1. **System description.** Consider a class of networked nonstrict-feedback nonlinear systems:

$$\begin{aligned}
&\dot{x}_k(t) = x_{k+1}(t) + f_k(x(t)), \quad k = 1, \ldots, n-1, \\
&\dot{x}_n(t) = u(t) + f_n(x(t)), \\
&y(t) = x_1(t),
\end{aligned} \tag{1}$$

where $x_k(t) \in \mathbb{R}$ are the system state and $x(t) = [x_1(t), \ldots, x_n(t)]^T$, $u(t) \in \mathbb{R}$ is the control input, $y(t) \in \mathbb{R}$ is the system output, and $f_k(x) \in \mathbb{R}$ is the known continuous function.

Assumption 2.1. *The nonlinear function* $f_k(x(t))$, $k = 1, \ldots, n$, *satisfies*

$$|f_k(x(t))| \leq \alpha_k \sum_{i=1}^{k} |x_i(t)|,$$

where $\alpha_k \geq 0$ *are known constants.*

Let

$$\zeta_k = \frac{x_j}{\mu^{k-1}},\ v = \frac{u}{\mu^n}, \tag{2}$$

where $\mu \geq 1$ is a scalar. Then, system (1) can be rewritten as

$$\begin{aligned} &\dot{\zeta}_k(t) = \mu\zeta_{k+1}(t) + g_k(\zeta(t)), \quad k = 1, \ldots, n-1, \\ &\dot{\zeta}_n(t) = \mu v(t) + g_n(\zeta(t)), \\ &y(t) = \zeta_1(t), \end{aligned} \tag{3}$$

where $\zeta(t) = [\zeta_1(t), \ldots, \zeta_n(t)]^T$ and $g_k(\zeta(t)) = \frac{f_k(x(t))}{\mu^{k-1}}$. With the help of (2) and Assumption 2.1, we have

$$|g_k(\zeta(t))| \leq \alpha_k \sum_{i=1}^{k} |\zeta_i(t)|. \tag{4}$$

It follows from (3) that

$$\begin{aligned} &\dot{\zeta}(t) = \mu A\zeta(t) + \mu Bv(t) + G(\zeta(t)), \\ &y(t) = C\zeta(t), \end{aligned} \tag{5}$$

where

$$A = \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ & & & 0 \end{bmatrix},\ B = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix},\ C = \begin{bmatrix} 1 \\ \vdots \\ 0 \\ 0 \end{bmatrix}^T,\ G(\zeta(t)) = \begin{bmatrix} G_1(\zeta(t)) \\ \vdots \\ G_{n-1}(\zeta(t)) \\ G_n(\zeta(t)) \end{bmatrix}.$$

2.2. **DoS attacks.** Since the signal is transmitted through the network medium, network attacks may occur to interrupt the signal transmission. Here, the specific attack type we consider is DoS attacks. In order to achieve the main results of this paper, the following assumptions are required for the constraints of attack frequency and duration.

Assumption 2.2 (Attack Frequency)**.** *For* $t \geq t_1 \geq 0$, *there is a scalar* $T_0 > 0$, *such that*

$$N(t, t_1) \leq \frac{t - t_1}{T_0}.$$

Assumption 2.3 (Attack Duration)**.** *For* $t \geq t_1 \geq 0$, *there is a scalar* $T_1 > 1$, *such that*

$$\Pi(t, t_1) \leq \frac{t - t_1}{T_1}.$$

2.3. **Observer-based control design.** Let h be the sampling period and $t_j = jh$, $j = 0, 1, \ldots$, be the sampling instants. Then, the output signal of the sensor can be expressed as

$$y(t) = y(t_j),\ t \in [t_j, t_{j+1}).$$

Let the intervals $D_{1,j} = [d_j, d_j + l_j)$ and $D_{2,n} = [d_j + l_j, d_{j+1})$, $j = 0, 1, \ldots$, with $d_0 = 0$ be the non-attacking interval and the attacking interval, respectively. In addition, we assume that there exist integers κ_j and $\bar{\kappa}_j$, such that $d_j = \kappa_j h$ and $l_j = \bar{\kappa}_j h$. The subintervals on $D_{1,j}$ can be expressed as $D_{1,j} = \cup_{i=1}^{i_j^*} \Omega_j^i$, where $\Omega_j^i = [d_j + (i-1)h, d_j + ih)$

with $i_j^* = \frac{d_{j+1}-d_j}{h}$. Affected by DoS attacks, the actual expression of the observer's input is

$$\bar{y}^{\sigma(t)}(t) = \begin{cases} y(t), & t \in D_{1,j},\ \sigma(t) = 1, \\ 0, & t \in D_{2,j},\ \sigma(t) = 0. \end{cases} \tag{6}$$

According to (5) and (6), we can design the following state observer:

$$\begin{aligned} \dot{\hat{\zeta}}_k(t) &= \mu\hat{\zeta}_{k+1}(t) - \mu L_j^{\sigma(t)}\left(\zeta_1(t) - \bar{y}^{\sigma(t)}(t_k)\right), \quad k = 1, \ldots, n-1, \\ \dot{\hat{\zeta}}_n(t) &= \mu v(t) - \mu L_n^{\sigma(t)}\left(\zeta_1(t) - \bar{y}^{\sigma(t)}(t_k)\right), \end{aligned} \tag{7}$$

where the scalar $L_j^{\sigma(t)}$ is to be designed. Note that $\hat{x}_k(t) = \mu^{j-1}\hat{\zeta}_k(t)$. For simplify, we rewrite (7) as

$$\dot{\hat{\zeta}}(t) = \mu A_0^{\sigma(t)}\hat{\zeta}(t) + \mu Bv(t) + \mu\sigma(t)L^{\sigma(t)}C\zeta(t_k), \tag{8}$$

where $A_0^{\sigma(t)} = A - L^{\sigma(t)}C$ and $L^{\sigma(t)} = \left[L_1^{\sigma(t)^T}, \ldots, L_n^{\sigma(t)^T}\right]^T$. Under DoS attacks, the sampling-data controller is constructed as

$$v(t) = v^{\sigma(t)}(t) = \begin{cases} -K\hat{\zeta}(t_k), & t \in [t_k, t_{k+1}),\ \sigma(t) = 1, \\ 0, & t \in [t_k, t_{k+1}),\ \sigma(t) = 0, \end{cases} \tag{9}$$

where K is a gain matrix to be designed.

Let $\xi(t) = \left[\zeta^T(t)\ \hat{\zeta}^T(t)\right]^T$. Combining (5), (8), and (9), we get

$$\dot{\xi}(t) = \bar{A}_0^{\sigma(t)}\xi(t) + \bar{A}_1^{\sigma(t)}\xi(t-\tau(t)) + \bar{G}(\zeta(t)), \tag{10}$$

where $\bar{A}_0^{\sigma(t)} = \mu\text{diag}\left\{A, A_0^{\sigma(t)}\right\}$, $\bar{A}_1^{\sigma(t)} = \mu\left[\sigma(t)\bar{L}^{\sigma(t)}C\ \ -\bar{B}K^{\sigma(t)}\right]$, $\bar{L}^{\sigma(t)} = \left[\mathbf{0}\ L^{\sigma(t)}\right]^T$, $\bar{B} = \left[B^T\ B^T\right]^T$, $\bar{G}(\zeta(t)) = \left[G^T(\zeta(t))\ \mathbf{0}\right]^T$, $K^1 = K$, $K^0 = \mathbf{0}$, and $\tau(t) = t - t_j$. Assume that $\tau(t) < h$.

The objective of this work is to design an observer-based sampled-data controller, such that system (10) under DoS attacks is exponentially stable.

3. Main Results.

Theorem 3.1. *Let the gain matrices K, L^0 and L^1 be known. For given scalars $\mu \geq 1$, $\delta_l > 0$, $\beta_l > 0$, $T_0 > 0$, $T_1 > 1$, $\lambda_l > 1$, $l = 0, 1$, and $h > 0$, satisfying*

$$\varrho =: 2\beta_1 - 2(\beta_1 + \beta_0)\left(\frac{1}{T_1} + \frac{h}{T_0}\right) - \frac{\ln(\lambda_0\lambda_1)}{T_0} > 0, \tag{11}$$

if there exist symmetric matrices $P_l > 0$, and $Q_l > 0$ such that

$$P_1 \leq \lambda_0 P_0,\ P_0 \leq \lambda_1 e^{2(\beta_1+\beta_0)h}P_1, \tag{12}$$

$$\begin{bmatrix} \Gamma_{11} & \Gamma_{12} & P_1 & h\bar{A}_0^{1^T}P_1 \\ * & \Gamma_{13} & \mathbf{0} & h\bar{A}_1^{1^T}P_1 \\ * & * & -I & hP_1 \\ * & * & * & \Gamma_{14} \end{bmatrix} < 0, \tag{13}$$

$$\begin{bmatrix} \Gamma_{01} & R_0 & P_0 & h\bar{A}_0^{0^T}P_0 \\ * & \Gamma_{02} & \mathbf{0} & \mathbf{0} \\ * & * & -I & hP_0 \\ * & * & * & \Gamma_{04} \end{bmatrix} < 0, \tag{14}$$

where

$$\Gamma_{11} = \text{He}\left\{P_1\bar{A}_0^1\right\} + 2\beta_1 P_1 + dI - e^{-2\beta_1 h}R_1,$$

$$\Gamma_{12} = P_1\bar{A}_1^1 + e^{-2\beta_1 h}R_1,\ \Gamma_{13} = -e^{-2\beta_1 h}(Q_1 + R_1),$$
$$\Gamma_{14} = \delta_1^2 R_1 - 2\delta_1 P_1,\ \Gamma_{04} = \delta_0^2 R_0 - 2\delta_0 P_0,$$
$$\Gamma_{01} = \mathrm{He}\left\{P_0\bar{A}_0^0\right\} - 2\beta_0 P_0 - R_0,\ \Gamma_{02} = -Q_0 - R_0,$$

then system (10) *is exponentially stable.*

Proof: Construct a Lyapunov-Krasovskii functional of the following form, for $\forall t \in \Omega_j^i$:

$$V_{\sigma(t)}(t) = \xi^T(t)P_{\sigma(t)}\xi(t) + e^{(-1)^{\sigma(t)}2\beta_{\sigma(t)}(t-t_j-(i-1)h)}\left(\bar{\tau} - \tau(t)\right)\xi^T(t-\tau(t))Q_{\sigma(t)}\xi(t-\tau(t))$$
$$+ h\int_{-\tau(t)}^{0}\int_{t+s}^{t} e^{(-1)^{\sigma(t)}2\beta_{\sigma(t)}(t-\theta)}\dot{\xi}^T(\theta)R_{\sigma(t)}\dot{\xi}(\theta)\mathrm{d}\theta\mathrm{d}s.$$

When $\sigma(t) = 1$, the time derivative of $V_1(t)$ is

$$\begin{aligned}\dot{V}_1(t) + 2\beta_1 V_1(t) \le{}& \xi^T(t)\left[P_1\bar{A}_0^1 + \bar{A}_0^{1^T}P_1 + 2\beta_1 P_1\right]\xi(t) + 2\xi^T(t)P_1\bar{A}_1^1\xi(t-\tau(t))\\ &+ 2\xi^T(t)P_1\bar{G}(\zeta(t)) - e^{-2\beta_1 h}x^T(t-\tau(t))Q_1 x(t-\tau(t))\\ &+ h^2\dot{\xi}^T(t)R_1\dot{\xi}(t) - he^{-2\beta_1 h}\int_{t-\tau(t)}^{t}\dot{\xi}^T(\theta)R_1\dot{\xi}(\theta)\mathrm{d}\theta. \end{aligned} \tag{15}$$

By virtue of Jenson's inequality, the term $\int_{t-\tau(t)}^{t}\dot{\xi}^T(\theta)R_{\sigma(t)}\dot{\xi}(\theta)\mathrm{d}\theta$ can be evaluated as

$$h\int_{t-\tau(t)}^{t}\dot{\xi}^T(\theta)R_{\sigma(t)}\dot{\xi}(\theta)\mathrm{d}\theta \le -(\xi(t) - \xi(t-\tau(t)))^T R(\xi(t) - \xi(t-\tau(t))). \tag{16}$$

By using (4), we have

$$|g_k(\zeta(t))|^2 \le \left(\alpha_k\sum_{i=1}^{k}|\zeta_i(t)|\right)^2 \le k\alpha_k^2\sum_{i=1}^{k}|\zeta_i(t)|^2,$$

from which it follows that

$$\begin{aligned}\left\|\bar{G}(\zeta(t))\right\|^2 &= \sum_{k=1}^{n}|g_k(\zeta(t))|^2 \le |\zeta_1(t)|^2\sum_{k=1}^{n}k\alpha_k^2 + |\zeta_2(t)|^2\sum_{k=2}^{n}k\alpha_k^2 + \cdots + |\zeta_n(t)|^2\sum_{k=n}^{n}k\alpha_k^2\\ &\le \sum_{k=1}^{n}k\alpha_k^2\sum_{k=1}^{n}|\zeta_k(t)|^2 = d||\zeta(t)||^2,\end{aligned} \tag{17}$$

where $d = \sum_{k=1}^{n}k\alpha_k^2$.

Due to $\left(P_1R_1^{-\frac{1}{2}} - \delta_1 R^{\frac{1}{2}}\right)^T\left(P_1R_1^{-\frac{1}{2}} - \delta_1 R^{\frac{1}{2}}\right) \ge 0$, where $\delta_1 > 0$ is a constant, we have

$$-P_1R_1^{-1}P_1 \le \delta_1^2 R_1 - 2\delta P_1. \tag{18}$$

Then, integrating (15)-(18) and using (13), we have

$$\dot{V}_1(t) + 2\beta_1 V_1(t) < 0, \quad t \in D_{1,j}. \tag{19}$$

When $\sigma(t) = 0$, the time derivative of $V_0(t)$ is

$$\begin{aligned}\dot{V}_0(t) - 2\beta_0 V_0(t) \le{}& \xi^T(t)\left[P_0\bar{A}_0^0 + \bar{A}_0^{0^T}P_0 - 2\beta_0 P_0\right]\xi(t) + 2\xi^T(t)P_0\bar{G}(\zeta(t))\\ &- x^T(t-\tau(t))Q_0 x(t-\tau(t)) + h^2\dot{\xi}^T(t)R_0\dot{\xi}(t)\\ &- h\int_{t-\tau(t)}^{t}\dot{\xi}^T(\theta)R_0\dot{\xi}(\theta)\mathrm{d}\theta.\end{aligned}$$

In view of $\sigma(t) = 1$, by using (14), one can obtain

$$\dot{V}_0(t) - 2\beta_0 V_0(t) < 0, \quad t \in D_{2,j}. \tag{20}$$

Let

$$V(t) = \begin{cases} V_1(t), & t \in D_{1,j}, \\ V_0(t), & t \in D_{2,j}. \end{cases}$$

Then, it is clear that

$$\dot{V}(t) = \begin{cases} e^{-2\alpha_1(t-d_j)}V_1(d_j), & t \in D_{1,j}, \\ e^{2\alpha_0(t-d_j-l_j)}V_0(d_j + l_j), & t \in D_{2,j}. \end{cases}$$

The remaining proofs can be completed with the help of [11]. Therefore, the details are omitted.

Based on the result of Theorem 3.1, we give a sufficient condition of stability for system (10) and solve the control gain and observation gains.

Theorem 3.2. *For given scalars $\mu > 1$, $\rho > 0$, δ_l, $\beta_l > 0$, T_l, $\lambda_l > 1$, $l = 0, 1$, and $h > 0$, satisfying* (11)*, if there exists a constant $\phi > 0$, and symmetric matrices $P_l = \operatorname{diag}\{P_{l1}, P_{l2}\} > 0$, $Q_l > 0$, X_l and Y, such that*

$$\begin{bmatrix} -\phi I & (P_{11}B - BY)^T \\ * & -I \end{bmatrix} < 0 \tag{21}$$

$$P_1 \le \lambda_0 P_0, \ P_0 \le \lambda_1 e^{2\beta_1 h} P_1, \tag{22}$$

$$\begin{bmatrix} \bar{\Gamma}_{11} & \bar{\Gamma}_{12} & P_1 & h\mathcal{A}_1^T \\ * & \Gamma_{13} & \mathbf{0} & h\mathcal{A}_2^T \\ * & * & -I & hP_1 \\ * & * & * & \Gamma_{14} \end{bmatrix} < 0, \tag{23}$$

$$\begin{bmatrix} \bar{\Gamma}_{01} & R_0 & P_0 & h\mathcal{A}_0^T \\ * & \Gamma_{02} & \mathbf{0} & \mathbf{0} \\ * & * & -I & hP_0^T \\ * & * & * & \Gamma_{04} \end{bmatrix} < 0, \tag{24}$$

where

$$\begin{aligned} &P_{12} = \rho P_{11}, \ \mathcal{A}_1 = \operatorname{diag}\{P_{11}A, P_{12}A - X_1C\}, \\ &\bar{\Gamma}_{11} = \mu \operatorname{He}\{\mathcal{A}_1\} + 2\beta_1 P_1 + dI - e^{-2\beta_1 h} R_1, \\ &\bar{\Gamma}_{12} = \mu \mathcal{A}_2 + e^{-2\beta_1 h} R_1, \ \mathcal{A}_2 = \begin{bmatrix} \mathbf{0} & -B\bar{K} \\ \rho X_1 C & -\rho B\bar{K} \end{bmatrix}, \\ &\mathcal{A}_0 = \operatorname{diag}\{P_{01}A, P_{02}A - X_0C\}, \\ &\bar{\Gamma}_{01} = \mu \operatorname{He}\{\mathcal{A}_0\} + 2\beta_1 P_1 - 2\beta_0 P_0 - R_0, \end{aligned}$$

then system (10) *is exponentially stable. Furthermore, the observer gains and controller gain are given by*

$$L^1 = P_{12}^{-1}X_1, \ L^0 = P_{02}^{-1}X_2, \text{ and } K = Y^{-1}\bar{K}.$$

Proof: From system (5), we know that B is full column rank. Then, these exists a matrix Y such that $P_{11}B = BY$, which is equivalent to trace $\{(P_{11}B - BY)^T(P_{11}B - BY)\} = 0$. By using Schur complement, this condition can be transformed into an optimization problem (21). The proof is completed.

Remark 3.1. *In contrast to* [16]*, the main advantages of this paper are as follows: (I) we consider the scenario that DoS jamming signals simultaneously affect both forward and feedback channels, which may be more practical and (II) a new sampled-data controller is designed to guarantee that the underlying system under DoS attacks is exponentially stable. The observer and observer-based controller design results are expressed by the feasible* *solutions of the obtained LMIs, which can be solved by the standard LMI Toolbox. This method is simpler and easier to be implemented.*

4. A Numerical Example.

Consider the second-order nonlinear system

$$\begin{cases} \dot{x}_1(t) = x_2(t) - 0.1x_1(t)\sin\left(x_2^2(t)\right), \\ \dot{x}_2(t) = u(t) - 0.1x_2(t)\cos\left(x_1^2(t)\right). \end{cases} \tag{25}$$

Choose $h = 0.01$, $\mu = 1.1$, $\rho = 2$, $\lambda_0 = \lambda_1 = 1.01$, $T_0 = 2$, $T_1 = 3$, $\beta_0 = 0.8$, $\beta_1 = 0.5$, $\phi = 0.1$, and $\delta_0 = \delta_1 = 0.1$. By performing simple calculations, we get $d = 0.12$ and $\varrho = 0.1104$, which means that (11) holds. Then, by solving LMIs (21)-(24), we obtain

$$L^1 = \begin{bmatrix} 1.0735 & 0.2082 \end{bmatrix}^T, \ L^0 = \begin{bmatrix} 0.9970 & 0.8356 \end{bmatrix}^T, \text{ and } K = \begin{bmatrix} 0.3301 & 2.6587 \end{bmatrix}.$$

The following initial conditions are chosen: $x(0) = \begin{bmatrix} 1 & 2 \end{bmatrix}^T$, and $\hat{\xi}(0) = \begin{bmatrix} 1 & 0 \end{bmatrix}^T$. The state and control signals of system (25) are shown in Figures 1 and 2 from which we can observe that the effectiveness of the proposed method can be illustrated even if the system suffers from DoS attacks.

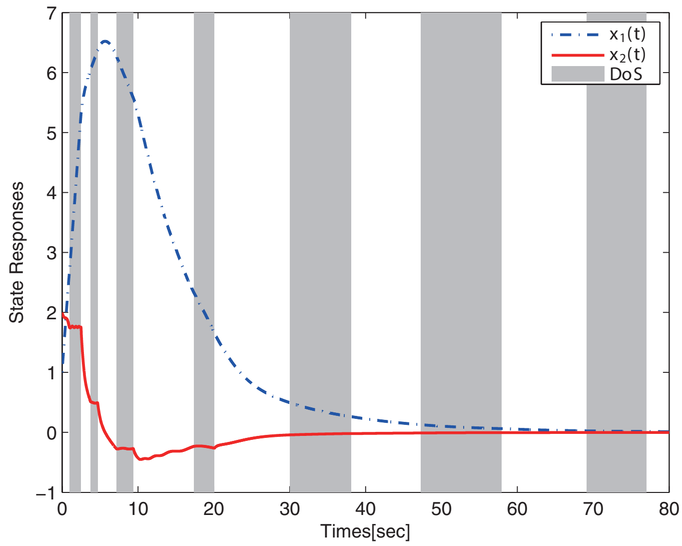

FIGURE 1. The states of system (25) under DoS attacks

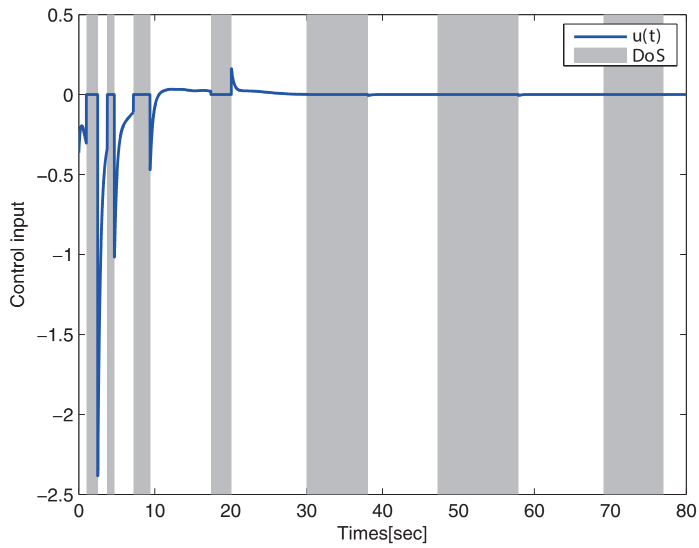

FIGURE 2. The control input of system (25) under DoS attacks

5. **Conclusions.** This paper has investigated sample-data control for networked non-strict-feedback nonlinear systems under aperiodic DoS jamming attacks. By using the intermittent output sampling information of the system, an observer and a controller that depend on the attack mode are designed. Sufficient conditions are obtained to ensure the investigated system under DoS jamming attacks to be exponentially stable. Finally, a numbercal example has been given to illustrate the effectiveness of the proposed method. Future study direction is to extend the presented control scheme of this article to large-scale networked systems.

Acknowledgment. This paper is funded by the International Exchange Program of Harbin Engineering University for Innovation-oriented Talents Cultivation.

REFERENCES

[1] J.-H. Guo and K.-L. Su, Intelligent security system based on power line communication, *ICIC Express Letters, Part B: Applications*, vol.8, no.2, pp.289-296, 2017.

[2] A. ur R. Jaffar, M. Nadeem, M. Alenezi and Y. Javed, Using public vulnerabilities data to self-heal security issues in software systems, *ICIC Express Letters*, vol.13, no.7, pp.557-567, 2019.

[3] S. Amin, G. A. Schwartz and S. S. Sastry, Security of interdependent and identical networked control systems, *Automatica*, vol.49, no.1, pp.186-192, 2013.

[4] H. Sandberg, S. Amin and K. H. Johansson, Cyber-physical security in networked control systems: An introduction to the issue, *IEEE Control Systems Magazine*, vol.35, no.1, pp.20-23, 2015.

[5] T. Okamoto, An immunity-enhancing security module for cloud servers, *International Journal of Innovative Computing, Information and Control*, vol.16, no.1, pp.137-151, 2020.

[6] S. Aoufi, A. Derhab and M. Guerroumi, Survey of false data injection in smart power grid: Attacks, countermeasures and challenges, *Journal of Information Security and Applications*, vol.54, pp.1-22, 2020.

[7] S. Amin, A. A. Cárdenas and S. S. Sastry, Safe and secure networked control systems under denial-of-service attacks, in *Hybrid Systems: Computation and Control. HSCC 2009. Lecture Notes in Computer Science*, R. Majumdar and P. Tabuada (eds.), Berlin, Heidelberg, Springer, 2009.

[8] H. S. Foroush and S. Martínez, On triggering control of single-input linear systems under pulse-width modulated DoS signals, *SIAM Journal on Control and Optimization*, vol.54, no.6, pp.3084-3105, 2016.

[9] C. D. Persis and P. Tesi, Input-to-state stabilizing control under denial-of-service, *IEEE Trans. Automatic Control*, vol.60, no.11, pp.2930-2944, 2015.

[10] A.-Y. Lu and G.-H. Yang, Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service, *IEEE Trans. Automatic Control*, vol.63, no.6, pp.1813-1820, 2018.

[11] N. Zhao, P. Shi, W. Xing and J. Chambers, Observer-based event-triggered approach for stochastic networked control systems under denial of service attacks, *IEEE Trans. Control of Network Systems*, vol.8, no.1, pp.158-167, 2021.

[12] N. Zhao, P. Shi and W. Xing, Dynamic event-triggered approach for networked control systems under denial of service attacks, *International Journal of Robust and Nonlinear Control*, vol.31, no.5, pp.1774-1795, 2021.

[13] C. Qian and H. Du, Global output feedback stabilization of a class of nonlinear systems via linear sampled-data control, *IEEE Trans. Automatic Control*, vol.57, no.11, pp.2934-2939, 2012.

[14] G. Sun, S. Xu and Z. Li, Finite-time fuzzy sampled-data control for nonlinear flexible spacecraft with stochastic actuator failures, *IEEE Trans. Industrial Electronics*, vol.64, no.5, pp.3851-3861, 2017.

[15] Y. Yuan, Y. Yu, Z. Wang and L. Guo, A sampled-data approach to nonlinear ESO-based active disturbance rejection control for pneumatic muscle actuator systems with actuator saturations, *IEEE Trans. Industrial Electronics*, vol.66, no.6, pp.4608-4617, 2019.

[16] S. Li, C. K. Ahn and Z. Xiang, Decentralized sampled-data control for cyber-physical systems subject to DoS attacks, *IEEE Systems Journal*, vol.15, no.4, pp.5126-5134, 2021.