Security and Safety, Vol. 2, 2023016 (2023)
https://doi.org/10.1051/sands/2023016
sands.edpsciences.org

Security and Safety in Unmanned Systems

Research Article

Open Access

Information Network

Communication security of autonomous ground vehicles based on networked control systems: The optimized LMI approach

Xiao Cai[1,*], Kaibo Shi[2,*], Kun She[3], Shouming Zhong[4], Shiping Wen[5], and Yuanlun Xie[3]

[1] *Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China*
[2] *School of Electronic Information and Electrical Engineering, Chengdu University, Sichuan 610106, China*
[3] *School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China*
[4] *School of Mathematics Sciences, University of Electronic Science and Technology of China, Chengdu 611731, China*
[5] *Faculty of Engineering and Information Technology, Australian AI Institute, University of Technology Sydney, Ultimo, NSW 2007, Australia*

Received: 2 January 2023 / Revised: 16 March 2023 / Accepted: 19 June 2023 / Published online: 23 August 2023

Abstract The paper presents a study of networked control systems (NCSs) that are subjected to periodic denial-of-service (DoS) attacks of varying intensity. The use of appropriate Lyapunov–Krasovskii functionals (LKFs) help to reduce the constraints of the basic conditions and lower the conservatism of the criteria. An optimization problem with constraints is formulated to select the trigger threshold, which is solved using the gradient descent algorithm (GDA) to improve resource utilization. An intelligent secure event-triggered controller (ISETC) is designed to ensure the safe operation of the system under DoS attacks. The approach is validated through experiments with an autonomous ground vehicle (AGV) system based on the Simulink platform. The proposed method offers the potential for developing effective defense mechanisms against DoS attacks in NCSs.

Keywords Networked control system, autonomous ground vehicle, cyber security, optimized LMI approach, event-trigger control

Citation Cai X, Shi K and She K et al. Communication security of autonomous ground vehicles based on networked control systems: The optimized LMI approach. Security and Safety 2023; **2**: 2023016. https://doi.org/10.1051/sands/2023016

1 Introduction

The 21st century has seen rapid development in network communication technology, which has revolutionized numerous fields, including industrial control. The integration of control theory, control technology, computer technology, and network communication technology has facilitated the growth of networked control systems (NCSs) [1, 2]. NCSs have been extensively utilized in diverse applications, as illustrated in Figure 1, and have emerged as the preferred technology due to the incorporation of communication and computer technology into the Internet-based TCP/IP protocol [3, 4].

The proposal of NCSs has allowed for the organic combination of regional control nodes and devices, breaking the information island phenomenon of traditional control systems. This approach expands the way information is transmitted and enables the diversification of management, monitoring, and control

* Corresponding authors (email: caixiao327327@163.com (Xiao Cai); skbs111@163.com (Kaibo Shi))

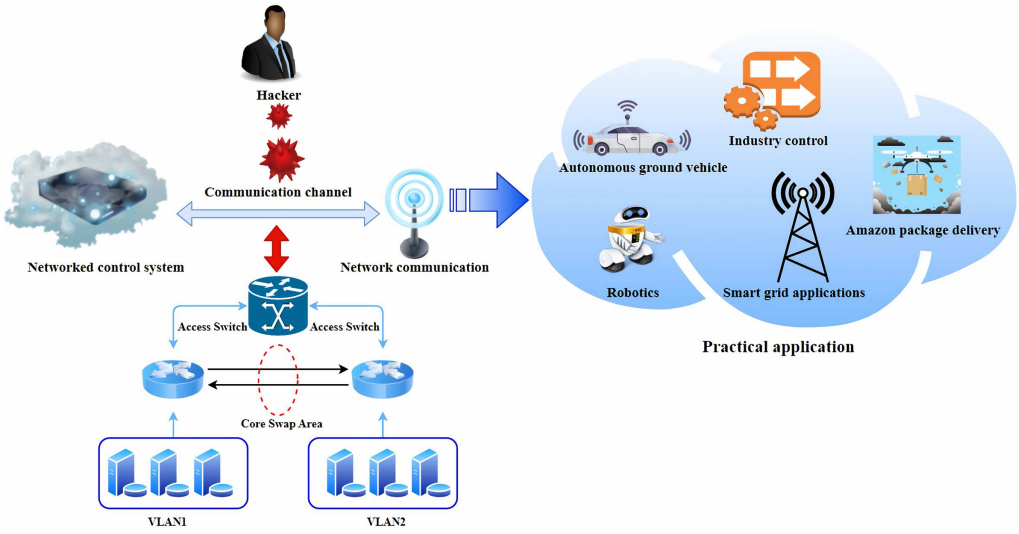

Figure 1. Networked control systems and application

strategies across different regions while simplifying the system's design and improving its reliability and flexibility [5, 6]. NCSs offer the favored development direction for future industrial control systems as they can add or delete control inputs and sensors as nodes are added or removed, offering the ability to modify and adapt the system to meet evolving requirements. Recent research on NCSs has focused on information transmission security, covert false data injection attacks, and network protocol and bandwidth selection to ensure that important closed-loop properties are maintained when inserting computer networks into feedback loops [7–9]. In [7], the author studied the information transmission security problem of NCSs. In [8], the design and detection of covert false data injection attacks against NCSs were studied from different perspectives of attackers and defenders. In [9], the authors investigated the choice of network protocols and bandwidth for NCSs to ensure that important closed-loop properties are preserved when inserting computer networks into feedback loops.

The security of NCSs can be classified into three main areas, namely information security, functional safety, and physical security [10]. Initially, functional and physical safety received more attention to prevent equipment or control system failures [11, 12]. Even in the event of equipment failure, the system should still be able to enter a safe, normal operating state. However, with the widespread adoption of Internet communication technology in industrial control systems, the significance of information security has become more prominent, and the industry has shifted its focus toward it [13]. Previous studies have proposed various approaches to mitigating the impact of denial-of-service (DoS) attacks on NCSs. For example, in [4], the authors proposed an improved approach to estimate performance errors caused by DoS attacks in T-S fuzzy NCSs using suitable integral elastic event-triggered mechanisms and improved Lyapunov–Krasovskii functionals (LKFs). In [14], a resilient event-triggered strategy was proposed for nonlinear NCSs with interval type-2 fuzzy models subject to nonperiodic DoS attacks, which aimed to reduce performance loss. The authors used a new mismatched membership function to simplify the network control structure under DoS attacks. In [15], an event-triggered control method was presented to analyze the impact of DoS attacks on NCSs in two cases: with and without DoS attacks. The authors in [16] proposed the security control problem of NCSs under DoS attacks as a critical research topic. Moreover, Cheng *et al.* [17] found that DoS attacks are periodic and studied the relationship between DoS periodic attacks and decay rates.

This paper proposes a periodic DoS attack with an attacking intensity and studies its impact on NCSs, building upon previous research. The study of DoS attacks is crucial for the security of NCSs due to the increasing prominence of information security issues resulting from the application and development of Internet communication technology in industrial control systems. As a result, there is a growing emphasis on information security in the industry, and researchers are actively developing strategies to mitigate the impact of DoS attacks on NCSs. Intelligent transportation systems heavily rely on autonomous ground vehicles (AGVs), which integrate various high-tech technologies that have been the subject of extensive

research [18, 19]. AGVs consist of multiple systems and technologies, including expert system planning functions, computer vision, autonomous navigation, and advanced parallel processing. AGVs can make independent judgments and plans, accept tasks in natural language, devise task execution methods, and continuously revise their plans. This design concept enables AGVs to complete tasks autonomously, even in complex terrain [20]. AGV control systems, as a new interdisciplinary field, can benefit from the use of NCSs, a novel type of control technology that relies on the Internet after the industrialized control system [21]. Therefore, combining NCSs with AGV control systems is an area of significant importance for research.

Based on the previous discussion, this paper focuses on the basic theory of NCSs and AGVs and conducts research on information security and intelligent secure event-triggered controller (ISETC) design issues for AGVs. The main contributions to this paper are summarized below:

(1) The paper proposes a model for NCSs under periodic DoS attacks with varying attack intensity. Suitable LKFs are constructed, and an optimized Linear Matrix Inequality (LMI) is used to analyze the stability of NCSs.
(2) The paper transforms the selection of the trigger threshold into an optimization problem with constraints and employs gradient descent algorithm (GDA) to optimize the threshold and ensure maximum utilization of sampling resources.
(3) An ISETC is designed for AGV's network communication. The ISETC is used to analyze the security and stability of the system and ensure that data transmission is not affected by malicious attacks.

Notation: $\mathrm{Sym}\{Q\}$ denotes $Q+Q^T$. $\mathbb{R}^{m\times n}$ denotes the set of $m\times n$ real matrices. I_n is the $n\times n$ identity matrix. $M>0(\geq 0)$ indicates M is a positive definite matrix. $\mathrm{diag}\{A_1, A_2, \ldots, A_n\}$ indicates a diagonal matrix and the diagonal elements are $A_i, i=1,2,\ldots,n$. P^{-1} indicates the inverse P. P^T is the transpose of matrix P. $\mathbb{R}^n$ is the n-dimensional Euclidean space.

2 Preliminaries

A. Event-trigger control and design of DoS attacks

In this paper, we focus on the study of NCSs that are subject to external disturbances as follows:

$$\dot{x}(t)=\mathscr{A}x(t)+\mathscr{B}u(t)+\mathscr{C}\omega(t), \tag{1}$$

where $x(t)\in\mathbb{R}^n$ means the current state vector; $u(t)\in\mathbb{R}^m$ is the signal to control the input; the external disturbance is $\omega(t)\in\mathfrak{L}_2[0,\infty)$; $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ are constant matrices.

In addition to external disturbances, this paper also examines the security of NCSs during network communication transmission. Specifically, we focus on the design of an ISETC to address DoS attacks that occur periodically and with varying levels of intensity. To model these attacks, we assume that the system is targeted by hackers at regular intervals, with t_kh representing the instantaneous sampling time point. The DoS attack design is based on prior research [22]:

$$\varphi_{t_{kh}}=\sum_{k=1}^{\infty}\mathscr{G}\delta(t-t_{kh}), \tag{2}$$

where $\mathscr{G}$ is attack intensity; $\delta(t-t_{kh})$ means Dirac function. The $S=\{t_kh\}_{k=1}^{\infty}$ and $\lim_{k\to\infty}t_kh=\infty$ is periodic attack signals. $\Delta x(t_kh)=x(t_k^+h)-x(t_k^-h)$, where $x(t_k^+h)=\lim_{\ell\to 0^+}x(t_kh+\ell)$ and $x(t_k^-h)=\lim_{\ell\to 0^-}x(t_kh+\ell)$. This paper assumes that $x(t)$ is right continuous, then we get $x(t_kh)=x(t_k^+)$ and has a left limit and the DoS attack interval is shown in Definition 1.

The ZOH function generates a sequence of control signals where the sampling instant t_kh satisfies $0=t_0<t_1h<t_2h<\cdots<t_kh<\cdots$, $t_{k+1}h$ $(k\in[0,\infty))$. Assuming that the sampling period satisfies $0\leq h_m<t_{k+1}h-t_kh\triangleq h_k\leq h_M$, and $\forall k\geq 0$. Then, we assume that $x(t_kh)$ is the value of the current state of the system thread; $x(t_k^*h)$ is the system thread state of the last successful transmission of the system. We have

$$e(t_kh)=x(t_k^*h)-x(t_kh), \tag{3}$$

where $e(t_kh)$ indicates the error between the current thread state of the system and the system thread state of the system's last successful transmission.

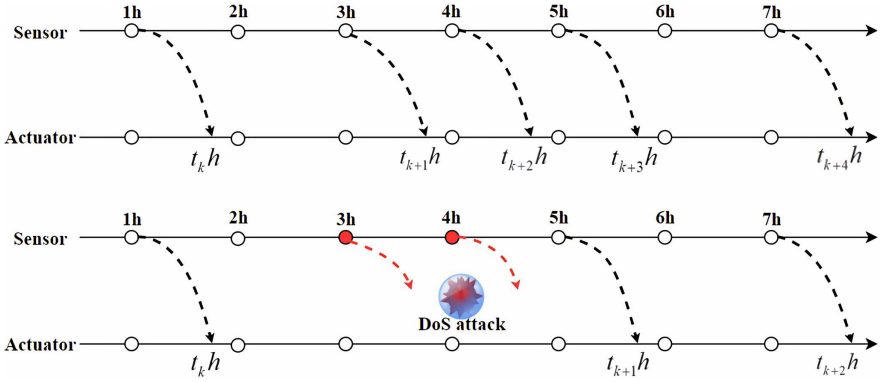

Figure 2. Event-trigger under DoS attacks

Attacks launched by hackers may cause errors in the trigger control of the system, as shown in Figure 2. To capture the impact of such attacks, we assume that $x(t_k^+ h + \sigma h)$ represents the system thread state at the last successful transmission following a DoS attack. The error is defined as follows:

$$e\left(t_k^+ h\right) = x\left(t_k^+ h + \sigma h\right) - x(t_k h), \tag{4}$$

where $\sigma \in \mathbb{N}$, $e(t_k h)$ represents the error between the current state of the system and the last successful transmission state when the hacker attacks.

Based on the above analysis, a new ETC is designed as follows [14]:

$$t_{k+1}^+ h = t_k h + \min_{\sigma}\{\sigma | \mathbf{\Theta} \geq 0\}, \tag{5}$$

where

$$\mathbf{\Theta} = e^T(t_k h)\Phi e(t_k h) + \varphi_{t_{kh}^+}\Upsilon\left(t_{k+1}^+ h\right) - \rho x(t_k h)\Phi x(t_k h),$$
$$\Upsilon\left(t_{k+1}^+ h\right) = e^T\left(t_k^+ h\right)\Phi e\left(t_k^+ h\right),$$

and $\Phi > 0$ is a weighting matrix; ρ indicates a threshold parameter; $\mathscr{G}$ means attack strength.

Defined the delay at every two successful sampling moments $\tau \triangleq t - t_k h$. Then, the control signal is designed as follows:

$$u(t) = \mathscr{K} x(t_k h),\ t \in \left[t_k h, t_{k+1}^+ h\right). \tag{6}$$

Based on the analysis of (1)–(5), we can get the following NSCs:

$$\dot{x}(t) = \mathscr{A} x(t) + \mathscr{B}\mathscr{K} x(t_k h) + \mathscr{C}\omega(t),\ t \in \left[t_k h, t_{k+1}^+ h\right), \tag{7}$$

where $\mathscr{K}$ is a controller gain matrix.

Remark 1. We considered the vulnerabilities of the ISETC in the presence of external attacks and proposed a novel approach to mitigate the effects of a periodic DoS attack $\phi_{t_{kh}}$ with varying strengths $\mathscr{G}$. Unlike the existing methods proposed in [15, 23], our approach takes into account the attack's periodicity and strength, which has important implications for developing effective defense mechanisms. By studying the behavior of the system under such attacks, we were able to design a robust and secure ISETC that provides reliable communication in the presence of adversarial interference.

B. Parameter optimization based on gradient descent algorithm

Selecting an appropriate threshold parameter ρ is a crucial aspect of trigger threshold design. The optimization of trigger threshold selection is a complex problem that can be formulated as an optimization problem with constraints. Based on optimization methods in several studies [24, 25], we also propose an optimal scheme for designing and optimizing trigger threshold selection. The main objective of the

scheme is to maximize the utilization of the available sampling resources, subject to the satisfaction of system performance and stability constraints. The following constraint problem is posed:

$$\begin{cases} \max\limits_{x\in\mathbb{R}^n} F(\rho), \\ \quad \text{s.t. } g_k(\rho) \le 0, k = 1, \cdots, r, \\ \qquad \rho^l \le \rho \le \rho^u, \end{cases} \tag{8}$$

where ρ is the threshold parameter that needs to be determined. $F(\rho) : \mathbb{R}^n \longrightarrow \mathbb{R}$ is the objective function. $g(\rho) : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ denotes a vector function for solving inequality constraint problems at ρ. ρ^l and ρ^u represent the upper and lower bounds of ρ, respectively.

Then, the gradient descent method is used to optimize the target problem by updating the threshold parameter iteratively. At each iteration, the step length is set as $\rho_{k+1} = \rho_k + m_k$, where m_k is the step size and $l_k\rho_k$ is the descent direction. The optimal threshold parameter is obtained when the objective function reaches its minimum value.

The parameter ρ_k is necessary for Pareto optimization, as there is no first-order descending direction for all individual goals. For all individual goals, there is no first-order descending direction as follows:

$$\text{range}(\nabla T_H(\rho_k)) \cap \left(-\mathbb{R}_+^n\right) = \emptyset, \tag{9}$$

where $\mathbb{R}_+^n$ is said to the pyramid, $T_H(\rho_k)$ is H in ρ_k of the jacobian matrix. When $n = 1$, $l_k = -\nabla h_1(\rho_k)$ for the fastest decline in the direction, which is equivalent to minimizing threshold $\nabla h_1(\rho_k)l + \frac{1}{2}||l||^2$ in l.

$$\begin{cases} (l_k, \nu_k) \in \underset{l\in\mathbb{R}^n,\nu\in\mathbb{R}}{\arg\max}\ \nu + \dfrac{1}{2}\|l\|^2, \\ \quad \text{s.t. } \nabla h_i(\rho_k)^\top l - \nu \le 0, \qquad \forall i = 1, \cdots, m. \end{cases} \tag{10}$$

It is proved that the dual of (10) is a sub-problem

$$\begin{cases} \lambda_k \in \underset{\lambda\in\mathbb{R}^n}{\arg\max} \left\| \sum\limits_{i=1}^{n} \lambda_i \nabla h_i(\rho_k) \right\|^2, \\ \text{s.t. } \lambda \in \Delta^n, \end{cases} \tag{11}$$

where $\Delta^n = \{\lambda : \sum_{i=1}^n \lambda_i, \lambda_i \ge 0, \forall i \in \{1, \cdots, m\}\}$ is a simplex set. According to the theory in [25], we get the following

$$\exists \sigma \in \Delta^n \to g_k(\rho) = \sum_{i=1}^{n} \lambda_i \nabla h_i(\rho_k) = 0. \tag{12}$$

Remark 2. In accordance with the approach described in references [24, 25], selecting an appropriate threshold parameter ρ is crucial for Pareto maximization. To address this problem, we transform the process into an optimization problem, which enables us to iteratively determine the optimal threshold parameter that satisfies the system requirements. By employing the gradient descent algorithm, we accelerate the search for the threshold parameter, resulting in optimized parameters that reduce the trigger rate and save sampling resources. This method has been proven effective in expediting the search process and enhancing the system's performance.

The Pareto first-order stationary point, denoted as $\rho_k \in \mathbb{P}$, is obtained by solving the optimization problem in equation (8) using the proximal gradient algorithm. This iterative algorithm updates the estimate of the Pareto front using the gradient of the objective function and the proximal operator of the regularization term. The proximal operator enforces the constraint that the estimate of the Pareto front belongs to the feasible set $\mathbb{P}$. The algorithm continues to update the estimate of the Pareto front until convergence is achieved, which is determined by a stopping criterion based on the norm of the difference between successive estimates of the Pareto front. The algorithm also includes a step size parameter m_k, which controls the step size of the gradient descent update. This parameter is chosen using a backtracking line search that ensures the update decreases the objective function. The specific steps of the algorithm are as follows:

Algorithm 1: Select the trigger threshold ρ based on the GDA

Input: $\rho_k \in [\rho^l, \rho^u] \subseteq S$ *and a step size sequence* m_k
Output: ρ_{k+1}
begin
  for $k = 0, 1, \cdots$ **do**
    Compute the gradients
    $\exists \lambda \in \Delta^n \to g_k(\rho) = \sum_{i=1}^n \lambda_i \nabla h_i(\rho_k) = 0$
    Solve the objective function
    $\lambda_k \in \arg\max_{\lambda \in \mathbb{R}^n} \| \sum_{i=1}^n \lambda_i \nabla h_i(\rho_k) \|^2$
    $\lambda \in \{\lambda : \sum_{i=1}^n \lambda_i, \lambda_i \geq 0, \forall i = 1, \cdots, m\}$
    Iterative the next updates ρ_{k+1}
    $\rho_{k+1} = \mathbb{P}_S(\rho_k - m_k g_k(\rho))$
  end
end

Definition 1. [26] The average DoS attacks interval of the attack time sequence $\vartheta = \{t_1, \cdots, t_k, \cdots\}$ is equal to T_a if there exist $S_0 \geq 0$ and T_a, we can get the DoS attacks interval as follow:

$$\frac{T-t}{T_a} - S_0 \leq N_\vartheta(T,t) \leq \frac{T-t}{T_a} + S_0,$$

where $\forall T \geq t \geq 0$ and $N_\vartheta(T,t)$ is the total number of times the attack sequence ϑ has been hacked over the time period (t,T).

Lemma 1. *[27] Given a x satisfies $x : [a,b] \to \mathbb{R}^n$. And there are the arbitrary matrices N_1, N_2 and N_3 and the matrices $M > 0$. We can get the following inequality holds:*

$$-\int_a^b \dot{e}^T M \dot{e} \, \mathrm{d}s \leq \xi_i^T \Omega \xi_i,$$

where

$$\xi_1 = col\left\{e(b), e(a), \frac{1}{b-a}\int_b^a e \, \mathrm{d}s, \frac{2}{(b-a)^2}\int_a^b \int_a^u e(u) \, \mathrm{d}s \, \mathrm{d}u\right\},$$

$$\xi_2 = col\left\{e(b), e(a), \frac{1}{b-a}\int_b^a e \, \mathrm{d}s, \frac{2}{(b-a)^2}\int_a^b \int_a^s e(u) \, \mathrm{d}s \, \mathrm{d}u\right\},$$

$$\Omega = (b-a)\left(N_1 M^{-1} N_1 + \frac{1}{3} N_2 M^{-1} N_2 + \frac{1}{5} N_3 M^{-1} N_3\right) + \mathrm{sym}\{(N_1\vartheta_1 + N_2)\vartheta_2 + N_3\vartheta_3^i\},$$

$$\vartheta_1 = e_1 - e_2, \ \vartheta_2 = e_1 + e_2 - 2e_3, \vartheta_3^1 = e_1 - e_2 - 6e_3 + 6e_4, \ \vartheta_3^2 = e_1 - e_2 + 6e_3 - 6e_4.$$

3 Main results

In this section, we consider the scenario where the control gain matrix $\mathscr{K}$ is known and establish the asymptotic stability condition of the system under the designed safe trigger mechanism, which is presented in Theorem 1. We then proceed to design and solve the controller gain matrix in Theorem 2. To simplify the notation, we define the following symbols:

$$\alpha(t) = col\{x(t), x(t_k h), x(t_{k+1} h)\}, \ \underline{h}_k = t_{k+1} h - t_k, \ \overline{h}_k = t - t_k h, \ \Pi_1 = col\{e_4 - e_1\}, \ \Pi_2 = col\{e_1 - e_3\},$$
$$\Pi_3 = col\{e_1, e_3, e_4\}, \ \Pi_4 = col\{e_5, \mathbf{0}, \mathbf{0}\}, \ \Phi = col\{e_1 - e_2, e_1 + e_2 - 2e_6, e_1 - e_2 + 6e_6 - 12e_7\},$$

$$\xi(t) = col\left\{x(t), x(t-\tau), x(t_k h), x(t_{k+1} h), \dot{x}(t), \frac{1}{\tau}\int_{t-\tau}^t x(s) \, \mathrm{d}s, \right.$$
$$\left. \frac{1}{\tau^2}\int_{t-\tau}^t \int_u^t x(s) \, \mathrm{d}s \, \mathrm{d}u, e(t_k h), e^{dos}\left(t_k^+ h\right), \omega(t)\right\},$$

$$\bar{\mathscr{K}} = \mathrm{diag}\{\mathscr{K}, 3\mathscr{K}, 5\mathscr{K}\}, \ e_i = \begin{bmatrix} 0_{n\times(i-1)n} & I_{n\times n} & 0_{n\times(9-i)} \end{bmatrix}, \quad i = 1, 2, \cdots, 9.$$

Theorem 1. *Let h_M, h_m, and ρ be positive scalars. The NCSs given by (7) are asymptotically stable if there exist symmetric matrices $\mathscr{P}$, $\mathscr{H}$, any matrix of suitable dimension $\mathscr{M}$, $\mathscr{Q}$, and $\mathscr{Y}_n$ $(n = 1, 2, 3)$ that satisfy the following LMIs:*

$$\mathscr{P} \geq 0,\ \mathscr{H} > 0,\ \Xi \leq 0, \tag{13}$$

where

$$\begin{aligned}
\Xi &= \Xi_a + \mathrm{Sym}\{\Gamma\Delta\} + \boldsymbol{\Theta}\big(\Upsilon\big(t_{k+1}^{+}h\big)\big),\\
\Xi_a &= \mathrm{Sym}\big\{e_1^T\mathscr{P}e_5\big\} + e_5^T\mathscr{M}\Pi_1 - \Pi_2^T\mathscr{M}e_5 + \underline{h}_k\Pi_3^T\mathscr{Q}\Pi_3 + \tau e_5^T\mathscr{H}e_5 + \Omega,\\
\Omega &= \Phi\tilde{\mathscr{H}}\Phi,\ \Gamma = e_1^T\mathscr{Y}_1 + e_{10}^T\mathscr{Y}_2 + e_5^T\mathscr{Y}_3,\ \Delta = \mathscr{A}e_1 + \mathscr{B}\mathscr{K}e_3 + \mathscr{C}e_{10} - e_5,\\
\boldsymbol{\Theta}\big(\Upsilon\big(t_{k+1}^{+}h\big)\big) &= e_8^T\Phi e_8 + \mathscr{G}e_9^T\Phi e_9 - \sigma e_3^T\Phi e_3.
\end{aligned}$$

Proof. Given the LKFs candidate as

$$V(t) = \sum_{i=1}^{3} V_i(t), \tag{14}$$

where

$$\begin{aligned}
V_1(t) &= x^T(t)\mathscr{P}x(t),\\
V_2(t) &= (x(t) - x(t_kh))\mathscr{M}(x(t_{k+1}h) - x(t)) + \overline{h}_k\underline{h}_k\alpha(t)\mathscr{Q}\alpha(t),\\
V_3(t) &= \int_{t-\tau}^{t}(s - t + \tau)\dot{x}^T(s)\mathscr{H}\dot{x}(s)\,\mathrm{d}s.
\end{aligned}$$

We take the derivative of $V_i(t)$, and we get

$$\dot{V}_1(t) = 2x^T(t)\mathscr{P}\dot{x}(t), \tag{15}$$

$$\begin{aligned}
\dot{V}_2(t) &= \dot{x}(t)\mathscr{M}(x(t_{k+1}h) - x(t)) - (x(t) - x(t_kh))\mathscr{M}\dot{x}(t)\\
&\quad + \underline{h}_k\alpha^T(t)\mathscr{Q}\alpha(t) - \overline{h}_k\alpha^T(t) + 2\overline{h}_k\underline{h}_k\alpha^T(t)\mathscr{Q}[\dot{x}(t), \mathbf{0}, \mathbf{0}]^T,
\end{aligned} \tag{16}$$

$$\dot{V}_3(t) = \tau\dot{x}^T(t)\mathscr{H}\dot{x}(t) - \int_{t-\tau}^{t}\dot{x}^T(s)\mathscr{H}\dot{x}(s)\,\mathrm{d}s. \tag{17}$$

Using the integral inequality in Lemma 1, the integral term in (17) can be scaled as follows:

$$\begin{aligned}
-\int_{t-\tau}^{t}\dot{x}^T(s)\mathscr{H}\dot{x}(s)\,\mathrm{d}s \leq &-\begin{bmatrix} x(t) - x(t-\tau)\\ x(t) + x(t-\tau) - 2\int_{t-\tau}^{t}\frac{x(s)}{\tau}\,\mathrm{d}s\\ x(t) - x(t-\tau) + 6\int_{t-\tau}^{t}\frac{x(s)}{\tau}\,\mathrm{d}s - 12\int_{t-\tau}^{t}\int_{u}^{t}\frac{x(s)}{\tau^2}\,\mathrm{d}s\,\mathrm{d}u \end{bmatrix}^T\\
&\times\begin{bmatrix} \mathscr{H} & 0 & 0\\ 0 & 3\mathscr{H} & 0\\ 0 & 0 & 5\mathscr{H} \end{bmatrix}\begin{bmatrix} x(t) - x(t-\tau)\\ x(t) + x(t-\tau) - 2\int_{t-\tau}^{t}\frac{x(s)}{\tau}\,\mathrm{d}s\\ x(t) - x(t-\tau) + 6\int_{t-\tau}^{t}\frac{x(s)}{\tau}\,\mathrm{d}s - 12\int_{t-\tau}^{t}\int_{u}^{t}\frac{x(s)}{\tau^2}\,\mathrm{d}s\,\mathrm{d}u \end{bmatrix}.
\end{aligned} \tag{18}$$

Based on the above results, $\dot{V}_3(t)$ can be rewritten as follows:

$$\dot{V}_3(t) \leq \tau\dot{x}^T(t)\mathscr{H}\dot{x}(t) + \Omega. \tag{19}$$

The constraints of the unsafe ISETC (5) are considered, and the following inequality is obtained:

$$0 \leq e^T(t_kh)\Phi e(t_kh) + \mathscr{G}\Upsilon\big(t_{k+1}^{+}h\big) - \rho x(t_kh)\Phi x(t_kh) = \xi^T(t)\boldsymbol{\Theta}\big(\Upsilon\big(t_{k+1}^{+}h\big)\big)\xi(t). \tag{20}$$

Based on the system (7), the following equation is got

$$\begin{aligned}
0 &= 2\big[x^T(t)\mathscr{Y}_1 + \omega^T(t)\mathscr{Y}_2 + \dot{x}^T(t)\mathscr{Y}_3\big]\big[\mathscr{A}x(t) + \mathscr{B}u(t) + \mathscr{C}\omega(t) - \dot{x}(t)\big]\\
&= 2\big[x^T(t)\mathscr{Y}_1 + \omega^T(t)\mathscr{Y}_2 + \dot{x}^T(t)\mathscr{Y}_3\big]\big[\mathscr{A}x(t) + \mathscr{B}\mathscr{K}x(t_{kh}) + \mathscr{C}\omega(t) - \dot{x}(t)\big]
\end{aligned}$$

$$= \mathrm{Sym}\{\xi^T(t)\Gamma\Delta\xi(t)\}. \tag{21}$$

According to (14)–(21), the following equation is had as follow

$$\dot{V}_i(t) \leq \xi^T(t)\Xi\xi(t). \tag{22}$$

Based on the linear convex combinations method [28], for all $\xi^T(t)\Xi\xi(t) < 0$ are established. We can get

$$\Xi(t = t_k h) \leq 0,\ \Xi(t = t_{k+1}h) \leq 0. \tag{23}$$

Finally, we can conclude that the NCSs (7) are asymptotically stable if the conditions (11) of Theorem 1 are satisfied and if the inequality $\dot{V}_i(t) \leq \xi^T(t)\Xi\xi(t) \leq 0$ holds. This inequality ensures that the LKF $V(t)$ is decreasing along the system trajectory, and therefore, the system state will converge to the equilibrium point. Thus, the designed safe trigger mechanism ensures the asymptotic stability of the NCSs in the presence of DoS attacks.

Remark 3. Unlike the method in reference [29], the sampling time information is fully considered in the looped function constructed by $V_2(t)$. It contains both the date information on $x(t_k h)$ and $x(t_{k+1}h)$, satisfying $\lim_{t\to t_k^+ h} V_2(t) = \lim_{t\to t_k^- } V_2(t) = \lim_{t\to t_{k+1}^+ h} V_2(t) = \lim_{t\to t_{k+1}^- h} V_2(t) = 0$. This method introduces more sampling time information based on reducing the initial constraints. Furthermore, increasing the information storage of LKFs reduces the conservatism of the criteria.

Remark 4. Analyzing the computational complexity of control algorithms is essential. In this paper, a loop function is constructed to reduce the initial constraints and therefore decrease the computational complexity of the control algorithm. The resulting algorithm achieves effective control of AGVs with relatively low computational complexity, specifically $6n^2 + n$. Moreover, we were able to verify the results within an acceptable time using an Intel(R) Core(TM) i7-8565U CPU @ 1.80 GHz 1.99 GHz computer.

The control algorithm considers stability analysis and employs an optimization approach to determine the maximum allowable delay and the controller gain matrix. This guarantees the system's stability under DoS attacks while minimizing their impact on the system's performance. Control Algorithm 2 is based on the presented stability analysis, and it aims to calculate the maximum allowable delay $\tau_{\max}$ and the controller gain matrix K to ensure the system's stability under DoS attacks. The algorithm is outlined as follows:

Algorithm 2: The maximum acceptable time delay $\tau_{\max}$ and controller gain matrix $\mathscr{K}$

Input: *The known positive definite vector* ρ, h_m, h_M, μ_1, $\mathscr{G}$ *and* μ_2
Output: *The maximum acceptable time delay* $\tau_{\max}$ *and controller gain matrix* $\mathscr{K}$

1 *Initialize the global counter* δ_i;
2 *Reset maximum acceptable time delay* $\tau_{\max}$;
3 **for** $\delta_i = 0 : 0.0001 : 1$ **do**
4 $\mathscr{P} \geq 0,\ \mathscr{H} > 0,\ \Xi \leq 0,$
5 **if** *There is not a feasible solution* **then**
6 *Replace* $\tau_{\max}$ *with* $\tau_{\max} + \delta_i$;
7 *Replace* δ_i *with* δ_{i+1};
8 **Return** *Line 4*
9 **else break**
10 **end**
11 **end**

Theorem 2. *Let* ρ, μ_1, μ_2, h_m, *and* h_M *be positive scalars. Consider the NCSs* (7) *under the designed safe trigger mechanism. The system is asymptotically stable if there exist symmetric matrices* $\tilde{\mathscr{P}}$, $\tilde{\mathscr{H}}$, *and any matrices* $\tilde{\mathscr{M}}$, $\tilde{\mathscr{Q}}$, *and* $\mathscr{W}$ *that satisfy the following LMIs:*

$$\tilde{\mathscr{P}} \geq 0,\ \tilde{\mathscr{H}} > 0,\ \tilde{\Xi} \leq 0, \tag{24}$$

where

$$\tilde{\Xi} = \tilde{\Xi}_a + Sym\left\{\tilde{\Gamma}\tilde{\Delta}\right\} + \tilde{\mathbf{\Theta}}\left(\Upsilon\left(t_{k+1}^+ h\right)\right),$$

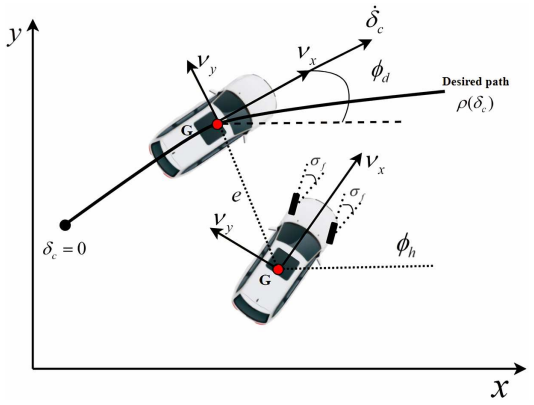

Figure 3. Schematic diagram of path following model

Table 1. Parameter values of the autonomous ground vehicles

Parameter	m	I_s	l_n	l_m	C_n	C_m
Value	1500	2500	1.3	1.4	40 000	40 000
Unit	kg	kg·	m	m	N/rad	N/rad

$$\tilde{\Xi}_a = Sym\Big\{e_1^T\tilde{\mathscr{P}}e_5\Big\} + e_5^T\tilde{\mathscr{M}}\Pi_1 - \Pi_2^T\tilde{\mathscr{M}}e_5 + \underline{h}_k\Pi_3^T\tilde{\mathscr{Q}}\Pi_3 + \tau e_5^T\tilde{\mathscr{H}}e_5 + \tilde{\Omega},$$
$$\tilde{\Omega} = \Phi\tilde{\bar{\mathscr{H}}}\Phi,\ \tilde{\Gamma} = e_1^T + \mu_1 e_{10}^T + \mu_2 e_5^T,\ \tilde{\Delta} = \mathscr{A}\mathscr{X}e_1 + \mathscr{B}\mathscr{W}e_3 + \mathscr{C}\mathscr{X}e_{10} - \mathscr{X}e_5,$$
$$\tilde{\bar{\mathscr{H}}} = diag\Big\{\tilde{\mathscr{H}}, 3\tilde{\mathscr{H}}, 5\tilde{\mathscr{H}}\Big\},$$
$$\tilde{\mathbf{\Theta}}\big(\Upsilon(t_{k+1}^+h)\big) = e_8^T\tilde{\Phi}e_8 + \mathscr{G}e_9^T\tilde{\Phi}e_9 - \sigma e_3^T\tilde{\Phi}e_3.$$

Proof. The gain matrix $\mathscr{K} = \mathscr{W}\mathscr{X}^{-1}$ and $\Phi = \mathscr{X}^{-T}\tilde{\Phi}X^{-1}$ are defined. Pre-multiplying and post-multiplying (13) by

$$\mathscr{Y}_1 = \mathscr{X}^{-1},\ \mathscr{Y}_2 = \mu_1\mathscr{X}^{-1},\ \mathscr{Y}_3 = \mu_2\mathscr{X}^{-1},\ \tilde{\mathscr{P}} = \mathscr{X}^T\mathscr{P}\mathscr{X},$$
$$\tilde{\mathscr{H}} = \mathscr{X}^T\mathscr{H}\mathscr{X},\ \tilde{\mathscr{Q}} = \mathscr{X}^T\mathscr{Q}\mathscr{X},\ \tilde{\mathscr{M}} = \mathscr{X}^T\mathscr{M}\mathscr{X}.$$

Then, the LMIs (23) can be obtained. The detailed proof process is similar to Theorem 1.

4 Illustrative example

We conducted simulation experiments on the Simulink joint platform to verify the effectiveness of the proposed control algorithm in this paper, using the data provided in reference [19]. The experimental setup is illustrated in Figure 3, and some data related to the vehicle are shown in Table 1:

The dynamic physics equations for AGV (see Figure 3) can be written as follows:

$$\begin{cases} \dot{e} = v_x\varpi + v_x\phi + s_1, \\ \dot{\phi} = r - \rho(\delta_c)v_x, \\ \dot{\varpi} = a_{11}\varpi + a_{22}r + b_1\sigma_n + s_2, \\ \dot{r} = a_{21}\varpi + a_{22}r + b_2\sigma_n + s_3. \end{cases}$$

Set the state vector is $x(t) = [e, \phi, \varpi, r]^T$, the control input signal is $u(t) = \sigma_f$ and the external disturbance $\omega(t) = [s_1, -\rho(\delta_c)v_x, s_2, s_3]^T$. Finally, the physical state space model of AGV is expressed as follows:

$$\dot{x}(t) = \mathscr{A}x(t) + \mathscr{B}u(t) + \omega(t),$$

Table 2. The maximum acceptable time delay $\tau_{\max}$ under different preset sampling periods h

h	Preset sampling periods				
	0.2	0.4	0.6	0.8	1.0
$\tau_{\max}$	1.7963	1.3821	1.1725	0.9974	0.5104

Table 3. The maximum acceptable time delay $\tau_{\max}$ under different DoS attack strength

DoS attacks	Preset attack strength				
	1	3	5	8	10
$\tau_{\max}$	2.3097	2.0715	1.7401	1.0092	0.5963

where

$$A=\begin{bmatrix} 0 & v_x & v_x & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -\frac{C_n+C_m}{mv_x^2} & -\left(1+\frac{l_nC_n+l_mC_m}{mv_x^2}\right) \\ 0 & 0 & \frac{l_nC_n+l_mC_m}{I_s} & -\frac{l_n^2C_n+l_m^2C_m}{v_xI_s} \end{bmatrix}, \quad B=\begin{bmatrix} 0 \\ 0 \\ \frac{C_n}{mv_x} \\ \frac{l_nC_n}{I_s} \end{bmatrix}.$$

The experimental setup was conducted on the Simulink joint platform to verify the effectiveness of the proposed control algorithm in this paper using the data provided in reference [19]. The physical meanings of the parameters were defined in [19]. Specifically, m denotes the weight of the vehicle, I_s is the yaw inertia of the vehicle, l_n represents the distance from the rear wheel to the center of gravity, l_m indicates the distance from the front wheel to the center of gravity, and C_n and C_m denote the cornering stiffness of the front and rear tires, respectively. We set the intensity to $\mathscr{G}=10$, with an attack period of 0.1, and assume that $h_m=0$ and $\rho=0.5$. To evaluate the impact of varying h_M on the system, we used the Yalmip toolbox to solve for the maximum acceptable time delay $\tau_{\max}$.

As shown in Table 2, the proposed control algorithm in this paper has a maximum acceptable delay limit of 1.3821 when $h_M=0.4$. In contrast, reference [19] limits the maximum acceptable latency to $\tau_{\max}=0.04$. This comparison clearly demonstrates the superior performance of the proposed algorithm in dealing with system delays and DoS attacks. The impact of DoS attacks on system performance is further studied, and we conduct simulations with different attack strengths and maximum delay constraints. Specifically, we set $h_M=0.2$ and examined the maximum acceptable delay of the DoS attack system under different attack strengths. The results are presented in Table 3, where we observe that the maximum acceptable time delay of the system changes with varying attack strengths. Notably, when the attack strength is set to $\mathscr{G}=10$, the maximum transmission time delay of the system is $\tau_{\max}=0.5963$. These results indicate the importance of implementing robust control strategies in NCSs that can handle and mitigate the effects of attacks, especially high-intensity DoS attacks. The proposed control algorithm in this paper has a computational complexity of $6n^2+n$, which means that the system's asymptotic stability can be ensured even with a low number of decision variables. Moreover, the low computational complexity of the control algorithm reduces processing time and energy consumption, making it more feasible for real-time control applications. In summary, the proposed control algorithm not only guarantees the system's stability and security but also provides practical benefits by minimizing the computational burden and optimizing resource allocation.

Then, the control gain matrix $K=10^4[2.0171\ -1.9720\ -0.9823\ -0.6937]$ was obtained using the method in Theorem 2 when the parameters μ_1 and μ_2 were set to 1. This control gain matrix was then used in a Simulink joint platform simulation experiment to verify the feasibility of the proposed control design method. The results presented in Figures 4 and 5 demonstrate that the proposed control design method is effective in mitigating the impact of DoS attacks on the system, as the system can still converge smoothly under the designed controller and control algorithm, even when subjected to DoS attacks with high intensity and a short attack period. Furthermore, the study found that the proposed control design method is more effective than the method presented in [19], as it enables the system to tolerate a higher maximum delay limit under DoS attacks, as shown in Table 2. These results provide valuable insights into

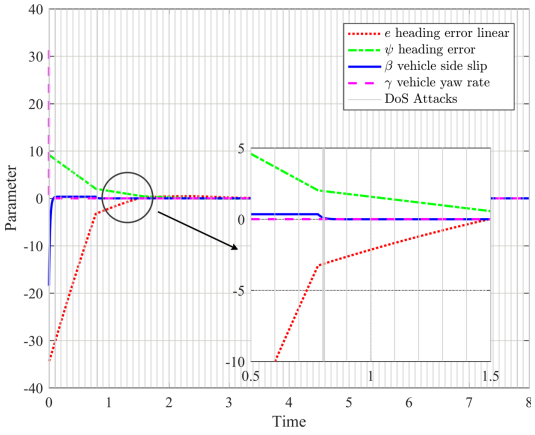

Figure 4. System parameter state trajectory response with DoS attacks

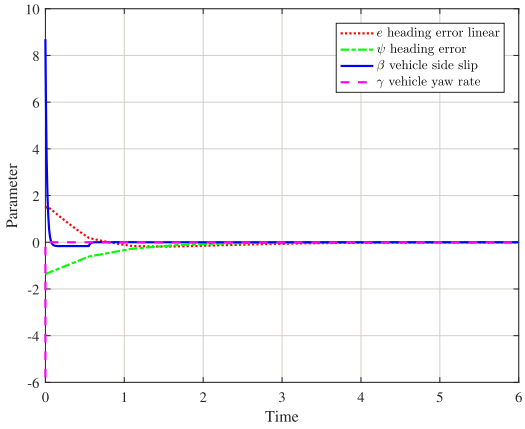

Figure 5. System parameter state trajectory response without DoS attacks

the development of robust control algorithms for NCSs that are vulnerable to DoS attacks, highlighting the importance of implementing such algorithms to ensure system stability and security. Additionally, the proposed control algorithm has relatively low computational complexity, making it a practical solution for real-time control applications.

Furthermore, selecting appropriate trigger thresholds is crucial for mitigating DoS attacks in practice. In this paper, we propose a novel approach based on GDA for optimizing trigger thresholds. By formulating the threshold selection as a constrained optimization problem, we can find optimal thresholds that minimize the trigger rate of legitimate traffic while maintaining high mitigation of DoS attacks. First, we iterate through the ρ_k values using the Python toolbox and then bring the results into the Yalmip toolbox for solving. This learning algorithm significantly improves resource efficiency by iteratively searching for a suitable value of ρ_k. The intelligent trigger threshold search mechanism employs machine learning to find the optimal threshold, denoted by ρ, by iteratively traversing the range $[0, 1]$ as shown in the sequence $\rho_1 \rightarrow \cdots \rightarrow \rho_2 \rightarrow \cdots \rightarrow \rho_{k-1} \rightarrow \cdots \rightarrow \rho_k \rightarrow \cdots$. In this way, the algorithm iteratively learns and searches for the ρ^k with the lowest trigger rate. Additionally, we present the number of system triggers under GDA and traditional algorithms are in Figures 6 and 7, respectively. Our results show that GDA-optimized thresholds can significantly reduce the number of false triggers compared to the conventional method, resulting in a lower trigger rate of 86.62% for GDA *versus* 88.5% for the traditional algorithm. These findings demonstrate the effectiveness of our proposed approach in reducing the impact of DoS attacks on network performance.

Finally, the optimized trigger thresholds can also provide additional benefits in terms of resource allocation and system resilience. By reducing the number of false triggers, our approach can free up more resources for other tasks or mitigate the impact of DoS attacks on system performance. In a word,

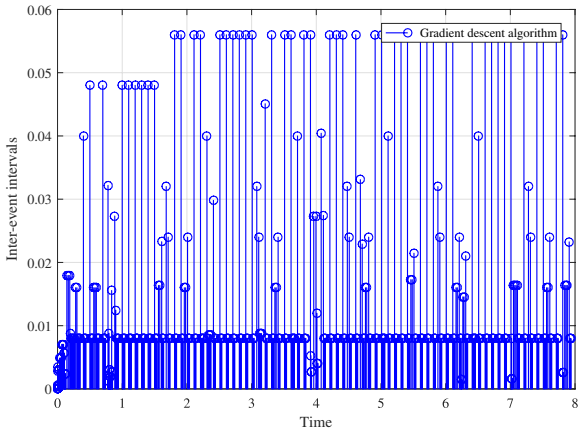

Figure 6. Release instants and time intervals under GDA

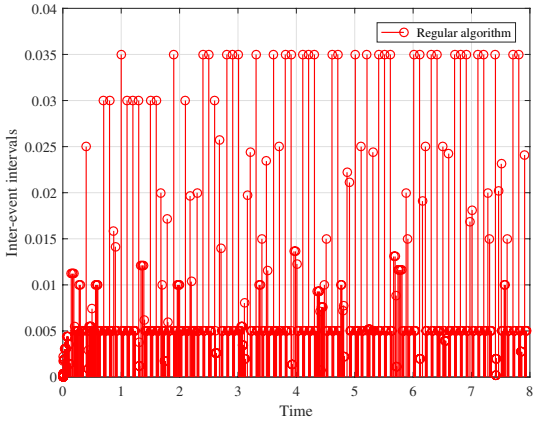

Figure 7. Release instants and time intervals under regular algorithm

our approach can enhance the security and reliability of network systems in the face of increasingly sophisticated DoS attacks.

5 Conclusion

This paper addressed the issue of NCSs under DoS attacks with periodicity and attack intensity. The research on the power of the DoS attacks was significant for establishing suitable defense mechanisms. The paper presented a method to construct appropriate LKFs, reducing the constraints of basic conditions and mitigating criterion conservatism. Additionally, the paper transformed the selection problem of the trigger threshold into an optimization problem with constraints and used the GDA to optimize the threshold, saving sampling resources. An ISETC was designed to ensure the normal operation of AGVs under DoS attacks. Finally, the proposed method's effectiveness was verified by simulating the AGVs system based on the Simulink platform. In the future, further research could focus on developing more sophisticated defense mechanisms to protect NCSs from different types of cyber-attacks and enhancing the performance and robustness of AGVs systems under various adverse conditions.

Conflict of Interest

No conflict of interest exists in the submission of this manuscript, and the manuscript is approved by all authors for publication. I would like to declare on behalf of my co-authors that the work described was original research that has not been published previously and is not under consideration for publication elsewhere, in whole or in part. All the authors listed have approved the manuscript that is enclosed.

Data Availability

We make data available on request through sending an email to the authors.

Authors' Contributions

Xiao Cai and Yuanlun Xie contributed to the conception of the study; Xiao Cai performed the experiment and the data analyses and wrote the manuscript; Kaibo Shi contributed significantly to the analysis and manuscript preparation; Kun She contributed significantly to the methodology and presentation of the manuscript; Shouming Zhong helped perform the analysis with constructive discussions.

Acknowledgements

We thank all anonymous reviewers for their helpful comments and suggestions.

Funding

This work was supported by the National Key Research and Development Plan (Grant No. 2020YFB2009503), the National Natural Science Foundation of China under Grant (Nos. 61703060, 61802036, 61701048, 61873305, U20B2046, 62272119, 62072130), the Sichuan Science and Technology Program under Grant No. 2021YJ0106, the Guangdong Basic and Applied Basic Research Foundation (Nos. 2020A1515010450, 2021A1515012307), Guangdong Province Universities and Colleges Pearl River Scholar Funded Scheme (2019), and Guangdong Higher Education Innovation Group (No. 2020KCXTD007), Guangzhou Higher Education Innovation Group (No. 202032854), Consulting project of the Chinese Academy of Engineering (2022-JB-04-05).

References

[1] Bemporad A, Heemels M and Johansson M. Networked Control Systems. Vol. 406. London: Springer, 2010.
[2] Gupta RA and Chow MY. Networked control system: overview and research trends. IEEE Trans Ind Electron 2009; **57**: 2527–35.
[3] Walsh GC and Ye H. Scheduling of networked control systems. IEEE Control Syst Mag 2001; **21**: 57–65.
[4] Cai X, Shi K and She K et al. Performance error estimation and elastic integral event triggering mechanism design for T-S fuzzy networked control system under DoS attacks. IEEE Trans Fuzzy Syst 2022; **31**: 1327–39.
[5] Wang F-Y and Liu D. Networked Control Systems. London: Springer, 2008.
[6] Zhang W, Branicky MS and Phillips SM. Stability of networked control systems. IEEE Control Syst Mag 2001; **21**: 84–99.
[7] Cai X, Shi K and She K et al. Quantized sampled-data control tactic for T–S fuzzy NCS under stochastic cyber-attacks and its application to truck-trailer system. IEEE Trans Veh Technol 2022; **71** 7023–32.
[8] Pang Z-H, Fan L-Z and Sun J et al. Detection of stealthy false data injection attacks against networked control systems via active data modification. Inf Sci 2021; **546**: 192–205.
[9] Walsh GC, Beldiman O and Bushnell LG. Asymptotic behavior of nonlinear networked control systems. IEEE Trans Autom Control 2001; **46**: 1093–97.
[10] Sandberg H, Amin S and Johansson KH. Cyberphysical security in networked control systems: an introduction to the issue. IEEE Control Syst Mag 2015; **35**: 20–3.
[11] Zeng W and Chow M-Y, Optimal tradeoff between performance and security in networked control systems based on coevolutionary algorithms. IEEE Trans Ind Electron 2011; **59**: 3016–25.
[12] Kogiso K and Fujita T. Cyber-security enhancement of networked control systems using homomorphic encryption. In: 2015 54th IEEE Conference on Decision and Control (CDC). IEEE, 2015, 6836–43.
[13] Zhang L, Gao H and Kaynak O. Network-induced constraints in networked control systems-a survey. IEEE Trans Ind Inf 2012; **9** 403–16.
[14] Pan Y, Wu Y and Lam H-K. Security-based fuzzy control for nonlinear networked control systems with DoS attacks via a resilient event-triggered scheme. IEEE Trans Fuzzy Syst 2022; **30**: 4359–68.
[15] Peng C and Sun H. Switching-like event-triggered control for networked control systems under malicious denial of service attacks. IEEE Trans Autom Control 2020; **65**: 3943–49.
[16] Amin S, Cárdenas AA and Sastry SS. Safe and secure networked control systems under denial-of-service attacks. In: Hybrid Systems: Computation and Control: 12th International Conference, HSCC 2009, San Francisco, CA, USA, April 13–15, 2009. Proceedings 12. Springer Berlin Heidelberg, 2009, 31–45.
[17] Hu S, Yue D and Xie X et al. Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks. IEEE Trans Cybern 2018; **49**: 4271–81.
[18] Ozguner U, Acarman T and Redmill KA, Autonomous Ground Vehicles. London: Artech House, 2011.
[19] Wang R, Jing H and Hu C et al. Robust H_∞ path following control for autonomous ground vehicles with delay and data dropout. IEEE Trans Intell Transp Syst 2016; **17**: 2042–50.
[20] Wu Y, Wang L and Zhang J. Path following control of autonomous ground vehicle based on nonsingular terminal sliding mode and active disturbance rejection control. IEEE Trans Veh Technol 2019; **68**: 6379–6390.
[21] Eskandarian A, Wu C and Sun C. Research advances and challenges of autonomous and connected ground vehicles. IEEE Trans Intell Transp Syst 2019; **22**: 683–711.
[22] He W, Qian F and Han Q-L et al. Almost sure stability of nonlinear systems under random and impulsive sequential attacks. IEEE Trans Autom Control 2020; **65**: 3879–86.
[23] Peng C and Sun H, Switching-like event-triggered control for networked control systems under malicious denial of service attacks. IEEE Trans Autom Control 2020; **65**: 3943–9.

[24] Plevris V and Papadrakakis M. A hybrid particle swarm-gradient algorithm for global structural optimization. Comput. Aided Civil Infrastruct Eng 2011; **26**: 48–68.
[25] Liu S and Vicente LN. The stochastic multi-gradient algorithm for multi-objective optimization and its application to supervised machine learning. Ann Oper Res 2021; 1–30, doi: 10.1007/s10479-021-04033-z.
[26] Lu J, Jiang B and Zheng WX, Potential impacts of delay on stability of impulsive control systems. IEEE Trans Autom Control 2021; **67** 5179–90.
[27] Cai X, Shi K and She K et al. Reliable sampling mechanism for Takagi–Sugeno fuzzy NCSs under deception cyberattacks for the application of the inverted pendulum system. IEEE Trans Reliab 2022, doi: 10.1109/TR.2022.3215075.
[28] Cai X, Shi K and She K et al. Event-triggered control strategy for 2-DoF helicopter system under DoS attacks. IEEE Trans Transp Electr 2023; **9** 3240–54.
[29] Hu S, Yue D and Xie X et al. Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks. IEEE Trans Cybern 2018; **49**: 4271–81.

Xiao Cai is currently a Ph.D. candidate at the University of Electronic Science and Technology of China, Chengdu, China. From September 2021 to September 2022, he was a visiting scholar with the Department of Electrical Engineering, Pohang University of Science and Technology, Pohang, South Korea. From November 2022 to November 2023, he is currently a visiting researcher with the School of Electrical & Electronic Engineering, Nanyang Technological University, Singapore. His current research interests include stability theorem, robustness stability, robust control, event trigger control, networked control systems, cyber-physical systems, optimized control and cyber security.

Kaibo Shi received a Ph.D. degree from the School of Automation Engineering, University of Electronic Science and Technology of China, Chengdu, China, in 2016. From September 2014 to September 2015, he was a Visiting Scholar with the Department of Applied Mathematics, University of Waterloo, Waterloo, ON, Canada. He was a Research Assistant with the Department of Computer and Information Science, Faculty of Science and Technology, University of Macau, Taipa, from May 2016 to June 2016 and January 2017 to October 2017. He is currently an Associate Professor at the School of Information Sciences and Engineering, at Chengdu University. His current research interests include the stability theorem, robustness stability, robust control, sampled-data control, synchronization, Lurie chatic system, stochastic systems, and neural networks.

Kun She received a B.Sc. degree in applied mathematics from the University of Electronic Science and Technology of China, Chengdu, Sichuan, China, in 1989, an M.Sc. degree in electronic and communication systems from the Southwest Institute of Communications, in 1992, and a Ph.D. degree in computer science from the University of Electronic Science and Technology of China. He is currently a Professor at the University of Electronic Science and Technology of China. Since 2006, he has been a Visiting Professor with the Illinois University of Technology. His research interests include intelligent computing, cloud computing, big data, network security, and network engineering.

Shouming Zhong was born in 1955. He received a graduate degree in applied mathematics in differential equations from the University of Electronic Science and Technology of China, Chengdu, China, in 1982. He has been a Professor at the School of Mathematical Sciences, University of Electronic Science and Technology of China since 1997. His current research interests include stability theorem and its application research of the differential system, robustness control, neural network, and biomathematics.

Shiping Wen (Senior Member, IEEE) received the MEng. degree in control science and engineering from School of Automation, Wuhan University of Technology, in 2010, and the Ph.D. degree in control science and engineering from the School of Automation, Huazhong University of Science and Technology, in 2013. He is currently a Professor at the Australian Artificial Intelligence Institute (AAII) at University of Technology Sydney. His research interests include memristor-based neural network, deep earning, computer vision, and their applications in medical informatics, *etc.*

Yuanlun Xie is currently working toward a Ph.D. degree in the School of Information and software engineering, University of Electronic Science and Technology of China. From November 2022 to November 2023, he is currently a visiting researcher with the School of Electrical & Electronic Engineering, Nanyang Technological University, Singapore. His main research interests include the algorithmic theory of machine learning, facial expression recognition by deep learning, and low-light image processing.