A Resilient Control Scheme for Networked Control Systems under Randomly Activated DoS Attacks

Wenyi Gao*

School of Electrical Engineering, University of Jinan, Jinan, China

*Corresponding author: gwy_gs@163.com

Abstract

In this paper, the elastic safety control problem of nonlinear active quarter vehicle suspension systems (AQVSSs) under random activation denial-of-service (DoS) attack is studied. Firstly, a class of networked discrete system model is established. Then, a DoS attack model with random activation is proposed, and a resilient controller is designed based on this model. Secondly, the augmented networked system model is derived, and the exponential stability of the system under the premise of H_∞ index is obtained by establishing the Lyapunov function. Finally, the advanced nature and theoretical value of the proposed algorithm are verified by simulation.

Keywords

Denial-of-service Attack; Networked Discrete System; Lyapunov Function.

1. Introduction

The benefits of networked control systems (NCSs), such as their high dependability, low maintenance costs, flexible design, and ease of installation, have drawn a lot of attention in recent years. Much effort has been put forward, and several significant outcomes have been attained [1]. NCSs achieve deep coupling between the network layer and the physical layer through a hybrid architecture of wireless and wired networks. Their open interconnection characteristics make the system face severe network attack threats, which may lead to multi-dimensional security risks such as control performance degradation, system stability damage, and even physical equipment damage [2], [3]. Therefore, the network security protection of NCSs has become one of the most challenging core issues in this field and has received extensive attention from academia and industry in recent years.

Generally speaking, the two primary categories of cyberattacks that are now in use are denial-of-service (DoS) attacks [4] and deception attacks [5], [6]. While the latter can stop access to system resources by blocking the communication channel, the former focuses on changing or impersonating packets in the network channel to jeopardize data confidentiality. For instance, Wang et al. [7] suggested a novel important-data-based DoS attack technique that uses packet importance to target the most "important" packets. As a result, it makes DoS attacks more damaging. Zhang et al. [8] developed an ideal jamming attack plan to optimize the linear quadratic Gaussian control cost function while taking the energy limitation into account. Therefore, it is necessary to propose a defense mechanism to effectively resist the impact of these malicious attacks.

Based on this, the innovative work of this paper is summarized as follows:

(1) A class of resilient controllers is designed according to the probabilistic properties of resilient DoS attacks triggered randomly.

(2) Under the premise of ensuring the performance index, a condition satisfying the exponential stability of the system is derived by considering the probability expectation property of the network attack in the stability proof.

2. Preparatory Knowledge and Model Description

2.1 Description of Discrete System Model

Consider the following discrete-time systems described by:

$$\begin{cases} x(h+1) = A^d x(h) + B^d u(h) + E^m \omega(h) \\ z(h) = C^d x(h) + D^d u(h) \end{cases} \tag{1}$$

where $x(h) \in \mathbb{R}^{n_x}$, $u(h) \in \mathbb{R}^{n_u}$, $z(h) \in \mathbb{R}^{n_z}$, $\omega(h) \in L_2[0,\infty)$ denote the system state, the control input, the control output and the unknown disturbance input, respectively. A^d, B^d, E^d, C^d, D^d, are known real matrices with suitable dimensions.

2.2 Description of DoS Attack and Controller Design

Due to the communication-open environment of Networked Control Systems (NCSs), the DoS attacks from the instrument to the controller would interfere with the control signal's transfer and change the measurement findings. However, because the opponent's energy is limited, it is extremely hard for attackers to constantly broadcast harmful signals in real-world applications. First, considering the unpredictability of DoS attacks, a Bernoulli variable $\mu(h)$ with a specific possibility is used to describe the unpredictable activating behavior of DoS attacks. The following definition of the attacked signal is thus presumed:

$$\bar{x}(h) = \mu(h)x(h) \tag{2}$$

which has the following properties:

$$\begin{aligned} &Prob\{\mu(h)=1\} = \bar{\mu}, Prob\{\mu(h)=0\} = 1-\bar{\mu} \\ &R\{\mu(h)\} = \bar{\mu}, R\{(\mu(h)-\mu^2\} = \bar{\mu}(1-\bar{\mu}) = \rho_\mu^2 \end{aligned} \tag{3}$$

where $Prob\{\mu(h)=1\}$ represents the probability that the Bernoulli variable is 1, $R\{\mu(h)\}$ represents the expectation of $\mu(h)$.

Specifically, when $\mu(h)=0$, it shows that the attack was successful at time h; when $\mu(h)=1$, it shows that the signal was sent without the DoS attack being active.

Different from the general controller, the fuzzy state-feedback controller is designed as follows:

$$u(h) = M(N)^{-1}\bar{x}(h) \tag{4}$$

where M, N are the gain matrix of the undetermined control variable.

By combining equations (1), (2), (4) and the probability expectation of DoS attack signal, we can obtain

$$\begin{aligned} &x(h+1) = (A^d + \bar{\mu}\Delta_1)x(h) + (\mu(h)-\bar{\mu})\Delta_1 x(h) + E^d \omega(h) \\ &z(h) = (C^d + \bar{\mu}\Delta_2)x(h) + (\mu(h)-\bar{\mu})\Delta_2 x(h) \end{aligned} \tag{5}$$

 Volume 11 Issue 5, 2025
DOI: 10.6919/ICJE.202505_11(5).0029

where $\Delta_1 = B^d M(N)^{-1}, \Delta_2 = D^d M(N)^{-1}$.

3. Main Results

Theorem 1: Given the Attenuation coefficient $\alpha > 1$, the positive scalar $\rho_\mu > 0$. M, N is the controller gain matrix. $\bar{\mu}$ is the given expectation of the Bernoulli variable. If there is a positive symmetric matrix $P > 0$ such that the system ensuring H_∞ performance is exponentially stable despite DoS attacks, then

$$\phi_\mu = \begin{bmatrix} \phi^{11} & * & * & * & * \\ G_1 & -P & * & * & * \\ \rho_\mu G_2 & 0 & -P & * & * \\ G_3 & 0 & 0 & -I & * \\ \rho_\mu G_4 & 0 & 0 & 0 & -I \end{bmatrix} < 0 \tag{6}$$

Where

$$\phi^{11} = \begin{bmatrix} -P^{-1} & * \\ 0 & -\gamma^2 I \end{bmatrix}, G_1 = \begin{bmatrix} \alpha(A^d + \bar{\mu}\Delta_1) & \alpha E^d \end{bmatrix}, G_2 = \begin{bmatrix} \alpha\Delta_1 & 0 \end{bmatrix}, G_3 = \begin{bmatrix} C^d + \bar{\mu}\Delta_2 & 0 \end{bmatrix}, G_4 = \begin{bmatrix} \Delta_2 & 0 \end{bmatrix}$$

Proof: Inspired by [9], this paper selects the following candidate functions for the Lyapunov function:

$$V(x(h)) = \alpha^{2h} x^T(h) P^{-1} x(h) \tag{7}$$

Using the forward difference to define the difference $\Delta V(x(h)) = V(x(h+1)) - V(x(h))$, we can get

$$R\{\Delta V(x(h))\} = \mathbb{R}\{\alpha^{2h+2} x^T(h+1) P^{-1} x(h+1) - \alpha^{2h} x^T(h) P^{-1} x(h)\} \tag{8}$$

Defining the augmented matrix $\delta(h) = \begin{bmatrix} x^T(h) & \omega^T(h) \end{bmatrix}^T$ as an augmented state vector, the following expression is further established:

$$\begin{aligned} &R\{\Delta V(x(h)) + \alpha^{2h}(\mathrm{z}^T(h)\mathrm{z}(h) - \gamma^2 \omega^T(h)\omega(h))\} \\ &= R\{\alpha^{2h}\delta^T(h)(\phi^{11} + G_1^T G_1 + \rho_\mu^2 G_2^T G_2 + G_3^T P^{-1} G_3 + \rho_\mu^2 G_4^T P^{-1} G_4)\delta(h)\} \\ &= R\{\alpha^{2h}\delta^T(h)\phi_\mu\delta(h)\} \le 0 \end{aligned} \tag{9}$$

When $\omega(h) = 0$, since $z^T(h)z(h) > 0$, it can be inferred from (9) that

$$R\{V(x(h+1)) - V(x(h))\} < 0 \tag{10}$$

Then we can further promote that

$$R\left\{V\left(x(h+1)\right)\right\} < R\left\{V\left(x(h)\right)\right\} < \cdots < R\left\{V\left(x(0)\right)\right\}. \tag{11}$$

Next, it is obtainable from (11) that

$$\alpha^{2h}\varepsilon_1 R\{\| x(h) \|^2\} < R\{V(x(h))\} < \varepsilon_2 \| x(0) \|^2 \tag{12}$$

where $\varepsilon_1 = \lambda_{\max}(P^{-1}), \varepsilon_2 = \lambda_{\min}(P^{-1})$, so

$$R\{\| x(h) \|\} < \sqrt{\frac{\varepsilon_1}{\varepsilon_2}}\alpha^{-h} \| x(0) \| \tag{13}$$

and the system (5) is exponentially stable.

In the presence of an external disturbance $\omega(h) = 0$, by adding the two sides of equation (9) from 0 to ∞ within the zero-initial condition, and due to $V\left(x\left(\infty\right)\right) > 0$, we can obtain that

$$E\{\sum_{h=0}^{\infty} z^T(h)z(h)\} \le \gamma^2 \sum_{h=0}^{\infty} \omega^T(h)\omega(h) \tag{14}$$

Define the matrix $J = diag\left\{N^T, I, I, I, I, I\right\}$, then pre and post-multiplying (6) by J and J^T, since $-N^T P^{-1} N \le P - N^T - N$, we can replace $-N^T P^{-1} N$ with $P - N^T - N$. Finally, an inequality for guaranteeing (6) can be obtained:

$$\phi_\mu = \begin{bmatrix} P - N - N^T & * & * & * & * & * \\ 0 & -\gamma^2 I & * & * & * & * \\ \alpha A^d N + \alpha\bar{\mu}B^d M & \alpha E^d & -P & * & * & * \\ \alpha\rho_\mu B^d M & 0 & 0 & -P & * & * \\ C^d N + \bar{\mu}D^d M & 0 & 0 & 0 & -I & * \\ \rho_\mu D^d M & 0 & 0 & 0 & 0 & -I \end{bmatrix} < 0 \tag{15}$$

4. Experimental Simulation Analysis

Table 1. Parameters of active suspension model.

Parameters	Definition	Value	Parameters	Value	Definition
k_s	stiffness of suspension	900 [N/m]	k_u	2500 [N/m]	compressibility of tire
m_s	sprung mass	2.45 [kg]	m_u	1 [kg]	unsprung mass
c_s	damping of suspension	7.5 [N·s/m]	c_u	5 [N·s/m]	damping of tire
$z_{\max}$	maximum displacement	0.038 [m]	$u_{\max}$	38.3 [N]	peak torque

In this part, relevant experimental tests are carried out to illustrate the superiority of the proposed control mechanism. The relevant parameters are set as follows: $\gamma = 50, \bar{\mu} = 0.8, \alpha = 1.0025$,and the suspension related parameters are shown in Table 1.

Considering Newton's second law in [9], [1], set $T_d = 0.001[\mathrm{s}]$, then the matrix parameters of the following active suspension system model and the state description of the suspension system are selected as follows:

$$x_1(h) = z_s(h) - z_u(h), x_2(h) = \dot{z}_s(h), x_3(h) = z_u(h) - z_r(h), x_4(h) = \dot{z}_u(h), z(h) = \ddot{z}_s(h) \quad (16)$$

$$A^d = T_d * \begin{bmatrix} 0 & 1 & 0 & -1 \\ -\frac{k_s}{m_s} & -\frac{c_s}{m_s} & 0 & \frac{c_s}{m_s} \\ 0 & 0 & 0 & 1 \\ \frac{k_s}{m_u} & \frac{c_s}{m_u} & -\frac{k_u}{m_u} & -\frac{c_s + c_u}{m_u} \end{bmatrix} + I, B^d = T_d * \begin{bmatrix} 0 \\ \frac{1}{m_s} \\ 0 \\ -\frac{1}{m_u} \end{bmatrix}, E^d = T_d * \begin{bmatrix} 0 \\ 0 \\ -1 \\ \frac{c_u}{m_u} \end{bmatrix}, \quad (17)$$

$$C^d = \begin{bmatrix} \frac{-k_s}{m_s} & -\frac{c_s}{m_s} & 0 & \frac{c_s}{m_s} \end{bmatrix}, D^d = \frac{1}{m_s}.$$

where the suspension deflection, sprung mass velocity, tire deflection, and unsprung mass velocity are shown by the symbols $x_1(h)$, $x_2(h)$, $x_3(h)$, and $x_4(h)$, respectively. The acceleration of the sprung mass is represented by the control output $z(h)$. The formula $w(h) = \dot{z}_r(h)$ is determined by applying the velocity input of the disruption.

By solving the linear matrix inequalities (LMIs) in Theorem 2, the controller gain matrix is calculated as follows:

$$M = \begin{bmatrix} 0.0103 & -0.0322 & -0.0003 & -0.0002 \end{bmatrix}$$

$$N = \begin{bmatrix} 1.1791*10^{-5} & -3.4556*10^{-5} & -3.6040*10^{-7} & 4.1269*10^{-7} \\ -3.4559*10^{-5} & 1.6756*10^{-4} & 1.0325*10^{-6} & -4.8861*10^{-6} \\ -3.6034*10^{-7} & 1.0316*10^{-6} & 3.5780*10^{-7} & -1.6314*10^{-6} \\ 4.0644*10^{-7} & -4.7891*10^{-6} & -1.6322*10^{-6} & 8.958*10^{-4} \end{bmatrix}$$

It can be observed from Fig. 1 that the suspension system still shows obvious superior performance even under attack. Specifically, although the four system states fluctuate under the attack state, the amplitude of the fluctuation does not increase significantly with time, indicating that the system has good anti-interference ability. In addition, the proposed algorithm can help the system effectively absorb and disperse the influence of road excitation, reduce the vertical displacement of the vehicle body, and significantly improve the ride comfort and stability of the vehicle.

It can be clearly seen from Fig. 2 that the body and tire under the passive suspension are always in a jitter state when facing the road pulse. Under the control of the algorithm proposed in this paper, the body and tire can respond quickly to pulse interference and recover smoothly. The actuator force and sprung mass acceleration under different conditions are shown in Fig. 3 and Fig. 4. This means that the control mechanism proposed in this paper can reduce the vertical acceleration of the suspension

 Volume 11 Issue 5, 2025
DOI: 10.6919/ICJE.202505_11(5).0029

while satisfying the actuator torque constraint. Thus, it provides a more comfortable driving experience.

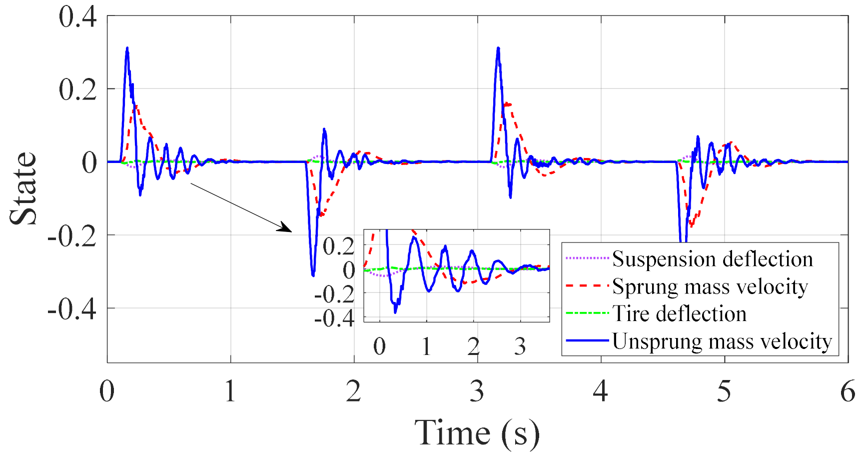

Fig. 1. Suspension system response curve during road excitation with impulse.

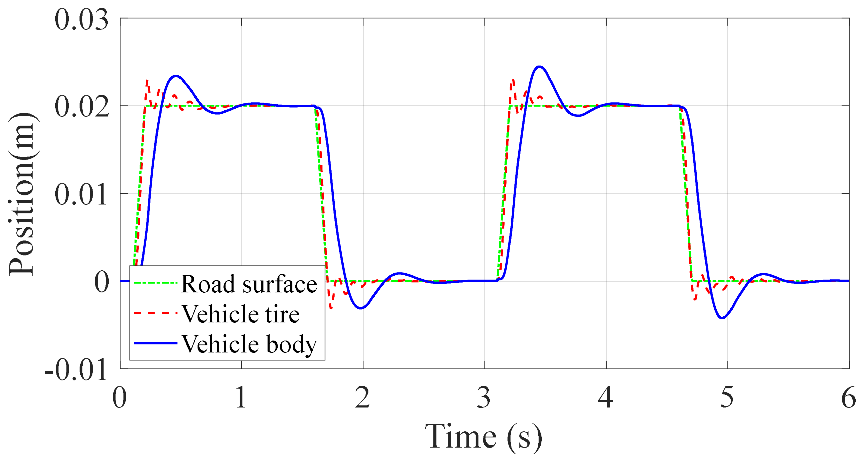

Fig. 2. Vertical displacement shifting on each pulsed road surface.

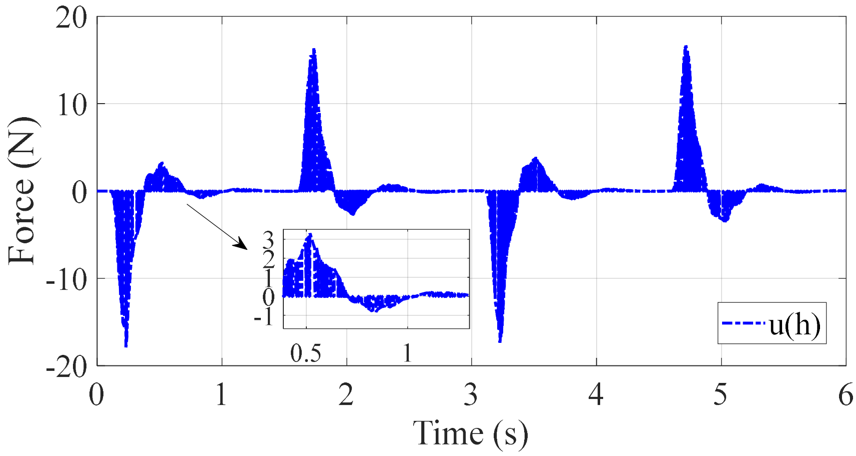

Fig. 3. Actuator force under DoS attacks.

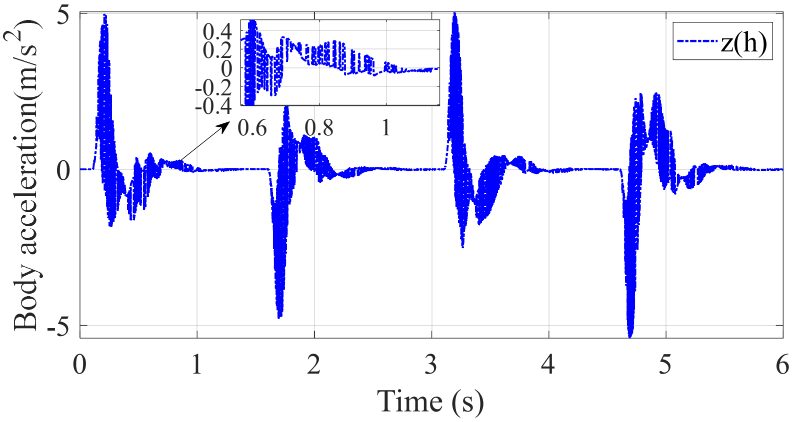

Fig. 4. Sprung mass acceleration under DoS attacks.

5. Conclusion

The elastic control mechanism proposed in this paper is effectively used to alleviate the impact of attacks on networked control systems. Through the experimental simulation of the real suspension system, it is verified that the proposed scheme has obvious advantages over the passive suspension and significantly improves the ride comfort of the driver. In the future, we will further discuss more extensive attack models in the field of action, and design a more complex and effective model to resist the impact of attacks.

References

[1] Shan Y, Xie X, Wu J, et al. Covert-Switching-Based Attack Mechanism and Resilient Observer-Assisted Control Strategy for Nonlinear Cyber-Physical Systems[J]. IEEE Internet of Things Journal, 2025, doi: 10.1109/JIOT.2025.3537582.

[2] Wang L, Wang Z, Wei G, et al. Observer-based consensus control for discrete-time multiagent systems with coding–decoding communication protocol[J]. IEEE Transactions on Cybernetics, 2018, 49(12): 4335-4345.

[3] Wang X, Wang X, Su H, et al. Coordination control for uncertain networked systems using interval observers[J]. IEEE transactions on cybernetics, 2019, 50(9): 4008-4019.

[4] Peixoto M L C, Coutinho P H S, Bessa I, et al. Event-triggered control of Takagi-Sugeno fuzzy systems under deception attacks[J]. International Journal of Robust and Nonlinear Control, 2023, 33(13): 7471-7487.

[5] Coutinho P H S, Bessa I, Pessim P S P, et al. A switching approach to event-triggered control systems under denial-of-service attacks[J]. Nonlinear Analysis: Hybrid Systems, 2023, 50: 101383.

[6] Wakaiki M, Cetinkaya A, Ishii H. Stabilization of networked control systems under DoS attacks and output quantization[J]. IEEE Transactions on Automatic Control, 2019, 65(8): 3560-3575.

[7] Wang X, Tian E, Zheng W X, et al. Important-data-based DoS attack mechanism and resilient H∞ filter design for networked T–S fuzzy systems[J]. IEEE Transactions on Cybernetics, 2023, 54(5): 3352-3362.

[8] Zhang H, Cheng P, Shi L, et al. Optimal DoS attack scheduling in wireless networked control system[J]. IEEE Transactions on Control Systems Technology, 2015, 24(3): 843-852.

[9] Shan Y, Xie X, Sun J, et al. Observer-based adaptive event-triggered control for nonlinear networked systems under multiple cyber attacks[J]. IEEE Transactions on Fuzzy Systems, 2024, doi: 10.1109/TFUZZ.2024.3418953.

[10] Shan Y, Xie X P, Sun N. Co-Design of Enhanced Fuzzy Observer-Based Estimation and Gain-Scheduling Control for Active Suspension Systems Under Malicious Attacks[J]. IEEE Transactions on Intelligent Transportation Systems, 2025, doi: 10.1109/TITS.2025.3535710.

[11] Sun H, Sun J, Chen J. Analysis and synthesis of networked control systems with random network-induced delays and sampling intervals[J]. Automatica, 2021, 125: 109385.