L_2-Gain-Based Path Following Control for Autonomous Vehicles Under Time-Constrained DoS Attacks

Songlin Hu, *Member, IEEE*, Yong Ma, *Member, IEEE*, Xin Qi, Zhixiong Li, *Senior Member, IEEE*, Reza Malekian, *Senior Member, IEEE*, and Miguel Angel Sotelo, *Fellow, IEEE*

***Abstract*— Autonomous vehicles (AVs) are being enhanced by introducing wireless communication to improve their intelligence, reliability and efficiency. Despite all of these distinct advantages, the open wireless communication links and connectivity make the AVs' vulnerability to cyber-attacks. This paper proposes an L_2-gain-based resilient path following control strategy for AVs under time-constrained denial-of-service (DoS) attacks and external interference. A switching-like path following control model of AVs is first built in the presence of DoS attacks, which is characterized by the lower and upper bounds of the sleeping period and active period of the DoS attacker. Then, the exponential stability and L_2-gain performance of the resulting switched system are analyzed by using a time-varying Lyapunov function method. On the basis of the obtained analysis results, L_2-gain-based resilient controllers are designed to achieve an acceptable path-following performance despite the presence of such DoS attacks. Finally, the effectiveness of the proposed L_2-gain-based resilient path following control method is confirmed by the simulation results obtained for the considered AVs model with different DoS attack parameters.**

Manuscript received 20 May 2022; revised 11 June 2023, 7 February 2024, and 30 May 2024; accepted 13 June 2024. Date of publication 12 July 2024; date of current version 29 August 2024. This work was supported in part by the National Natural Science Foundation of China under Grant 62173187, Grant 52261160383, and Grant 62073251; in part by the National Key Research and Development Plan under Grant 2023YFB4302300; in part by the Joint Fund of the Ministry of Education under Grant 8091B022239; in part by the Innovation Research Team Project of Hainan Natural Science Foundation under Grant 722CXTD518; in part by the Knowledge Innovation Program of Wuhan-Basic Research under Grant 2022010801010181; and in part by the National Science Centre of Poland under Project UMO-2023/51/B/ST8/02275. The Associate Editor for this article was S. Sacone. *(Corresponding authors: Yong Ma; Zhixiong Li.)*

Songlin Hu is with the Institute of Advanced Technology for Carbon Neutrality, Nanjing University of Posts and Telecommunications, Nanjing 210023, China (e-mail: songlin621@126.com).

Yong Ma and Xin Qi are with the State Key Laboratory of Maritime Technology and Safety and Hubei Key Laboratory of Inland Shipping Technology, School of Navigation, Wuhan University of Technology, Wuhan 430063, China, also with the Academician Workstation of China COSCO Shipping Corporation Ltd., Shanghai 200120, China, also with Sanya Science and Education Innovation Park, Wuhan University of Technology, Sanya 572000, China, and also with Chongqing Research Institute, Wuhan University of Technology, Chongqing 401120, China (e-mail: myongdl@whut.edu.cn; xinqi98@whut.edu.cn).

Zhixiong Li is with the Faculty of Mechanical Engineering, Opole University of Technology, 45-758 Opole, Poland (e-mail: zhixiong.li@ieee.org).

Reza Malekian is with the Department of Computer Science and Media Technology, Malmö University, 211 19 Malmö, Sweden (e-mail: reza.malekian@ieee.org).

Miguel Angel Sotelo is with the Department of Computer Engineering, University of Alcalá, Alcalá de Henares, 28801 Madrid, Spain (e-mail: miguel.sotelo@uah.es).

Digital Object Identifier 10.1109/TITS.2024.3422028

***Index Terms*— Path following, denial-of-service (DoS), L_2-gain, time-varying Lyapunov function, linear matrix inequality (LMI).**

I. Introduction

AUTONOMOUS vehicles (AVs) are rapidly developing form of intelligent transportation, with applications ranging from highways to dangerous battlefields [1]. Communication technology and autonomous vehicle integration are advancing new concepts in the field of mobile connectivity [2]. Advanced autonomous vehicle technologies and smart sensors are often structured to improve their safety and efficiency. However, because of the deep integration between communication and control, AVs are vulnerable to various attacks from the physical layer and the network layer [3], [4]. Therefore, in light of the vulnerabilities of the AV systems, it is imperative to evaluate their security controls for protection against interference and network attacks. Path-following control is the most basic subject of autonomous vehicle research. Its key task is to obtain the status and position information of the vehicle, which is then used to evaluate the tracking errors, and then to feedback them to the control system [5], [6]. For traditional vehicle operating stability control, scholars have proposed many control strategies, such as PID controllers [7], adaptive controllers [8], robust H_∞ controllers [9], MPC controllers [10] and Lyapunov functions [11]. However, in the course of signal transmission, given that a wide range of autonomous vehicle systems use open communication network, implying that the vehicles are vulnerable to cyber attacks. There is no doubt that a successful cyber attack on a self-driving vehicle could result in a deadly disaster at high speed [12]. Therefore, it is of paramount importance to investigate the resilient path following control problems that arise from the presence of cyber attacks [13].

In the real world, there are multiple types of cyber attacks on the AVs [14], [15], [16], with deception or false data injection (FDI) and DoS attacks being regarded as the most prevalent and devastating forms of attacks. FDI attacks mainly aim to tamper with communication network data to reduce the performance of the involved system [17]. DoS attacks are designed to interfere with communication channels to prevent information from being exchanged between vehicles [18], [19]. From a technical point of view, an attacker could perform a DoS attack by destroying the radio frequencies on wireless communication channels, resulting in congestion of those channels [20]. It is easier for the hackers to launch DoS attacks than to launch FDI attacks to some extent. In order to mitigate or eliminate the impacts of FDI or DoS attacks on AVs, a series of methods have been proposed in recent years. To mention a few, in [21], the authors develop a resilient control scheme to mitigate DoS attacks for networked vehicles equipped with collaborative adaptive cruise control. In [22], the authors propose a control-oriented vehicle system diagnostic framework, which can detect the occurrence of DoS attacks and also provide an estimate of the impact of the attacks. In [23], an attack detection method is proposed to protect the vehicle system from DoS attacks. In [24], a distributed secure platoon control strategy is proposed under DoS attacks.

There is no doubt that the research introduced above has achieved remarkable results but the design of a path-following control scheme for AVs in the presence of DoS attacks, as one of the most important of the basic driving tasks, has not received enough attention. And so far there have been few achievements in this field. In [25], an LMI-based path-following controller that was resilient against intermittent DoS attacks is developed. In [26], a novel self-discipline predictive control scheme for the path following of AVs subject to DoS attacks is proposed. Additionally, there are also some important results about path following control for AVs in the case of FDI attacks, see, e.g., [27] and [28]. It is worth pointing out that the DoS attack models considered in the above works restrict only the adversarial actions on the relevant attack duration and frequency, but it appears to be quite difficult to justify the incentive for a sophisticated real-world attacker to comply with such assumptions. From a practical perspective, it is more reasonable and imperative to develop an attack-resilient control approach that necessitates less knowledge of the concerned DoS attacks. To the best of the authors knowledge, this challenging issue has not been adequately addressed in the literature, not mentioning in the context of resilient path following control for AVs under partially known DoS attacks. This serves as the main motivation of this study.

Motivated by the above observations, this paper attempts to address the research gap regarding resilient path-following control for AVs under DoS attacks with partially known parameters. The main contributions of this paper are summarized as follows. (i) Different from the existing works such as [16], [25], and [26], a novel DoS off/on switching modeling framework is proposed for stability and L_2-gain analysis of the resilient path following control of AVs under a time-constraint DoS attacks; (ii) In contrast to the widely used time-invariant Lyapunov function approach as in [14], [15], [16], and [25], a time-varying Lyapunov function analysis method is proposed to analyze the stability and L_2-gain control synthesis of path-following control for AVs with DoS attacks by making use of the available DoS off/on characteristic parameters.

The rest of the paper is structured as follows. Section II mainly presents a path-following model, vehicle model, DoS attack model and control system model of AVs under DoS attacks. Based on the constructed model, the main results and algorithms are described in Section III. Section IV introduces the simulation, and its results verify the theoretical results. Section V provides some conclusions.

Notation: Throughout the paper, $\mathbb{R}^n$ denotes the n-dimensional Euclidean space. $\mathbb{R}^{n_c \times n}$ denotes the set of $n_c \times n$ real matrices. Symbol $*$ represents a symmetric term in a symmetric block matrix. $diag\{\cdots\}$ represents the block diagonal matrix. For the vector $x \in \mathbb{R}^n$, we express its 2-norm as $\|x\| = \sqrt{x^T x}$. In this article, matrices are assumed to have the appropriate dimensions unless explicitly stated.

II. Problem Formulation

A. Path Following Model

The path-following model of the autonomous vehicle is shown in Fig. 1. d represents the lateral deviation from the vehicles center of gravity to the nearest point Q on the desired path. The heading error e is defined as the error between the expected heading angle e_d and the actual heading angle e_h. r is the yaw angular velocity of the vehicle. δ_f is the front wheel steering angle. v_y and v_x are the lateral and longitudinal speeds of the vehicle, respectively. σ is the curvilinear coordinate of point Q along the path from the predefined initial position. $\rho(\sigma)$ represents the curvature of the expected path at point Q. The curvilinear coordinates of point Q along the path are defined as [29]

$$\dot{\sigma} = \frac{1}{1 - d \cdot \rho(\sigma)}(v_x \cos e - v_y \sin e) \tag{1}$$

Based on the Serret-Frenet equation in [30], the following path model of an AV is given as

$$\begin{cases} \dot{d} = v_x \sin e + v_y \cos e \\ \dot{e} = r - \rho(\sigma) v_x \end{cases} \tag{2}$$

Because the heading error ψ is small, the error d can be rewritten in the linear form as

$$\dot{d} = v_y + v_x e + d_0 \tag{3}$$

where d_0 represents the external disturbance and modeling error.

B. Vehicle Model

The vehicle planar motion model is shown in Fig. 2. Suppose the lateral forces of the front and rear wheels are F_f and F_r, then we have

$$F_f = C_f \alpha_f, \quad F_r = C_r \alpha_r \tag{4}$$

where C_f and C_r are the front and rear cornering stiffness values and α_f and α_r are the tire slip angles of the front and rear tires, which can be characterized by

$$\alpha_f = \delta_f - \frac{c_f r}{v_x} - \frac{v_y}{v_x}, \quad \alpha_r = \frac{c_r r}{v_x} - \frac{v_y}{v_x} \tag{5}$$

where c_f and c_r represent the center of gravity of the vehicle pointing to the front wheel and the rear wheel axis, respectively.

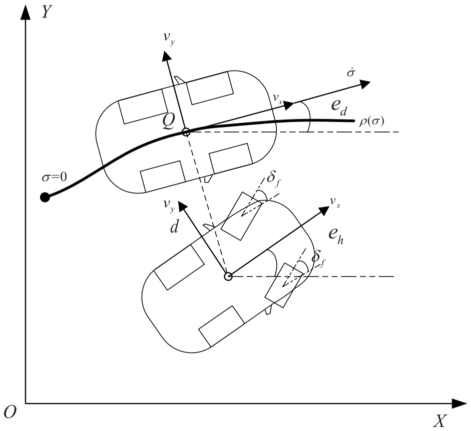


Fig. 1. Path following model.

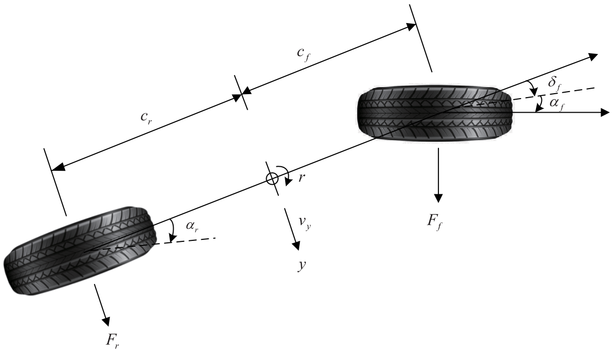


Fig. 2. Planar motion model.

Assuming that the front-wheel steering angle is small, the lateral dynamics of the vehicle can be characterized by

$$\begin{cases} \dot{\beta} = \dfrac{1}{m}(F_f + F_r) - r + d_1 \\ \dot{r} = \dfrac{1}{I}(c_f F_f - c_r F_r) + d_2 \end{cases} \tag{6}$$

where d_1 and d_2 represent external disturbances, I is the yaw inertia of the vehicle, m is the mass of the vehicle and β is the sideslip angle of the vehicle.

When the sideslip angle is small enough, we have $\beta = \frac{v_y}{v_x}$. Because the longitudinal velocity v_x is constant or the rate of change is slow, we can obtain $\dot{\beta} = \frac{\dot{v}_y}{v_x}$.

Based on the above descriptions, it follows from (6) that

$$\begin{cases} \dot{\beta} = a_{11}\beta + a_{12}r + b_0\delta_f + d_1 \\ \dot{r} = a_{21}\beta + a_{22}r + b_1\delta_f + d_2 \end{cases} \tag{7}$$

with $a_{11} = -\frac{(C_f+C_r)}{mv_x^2}, a_{12} = -(1 + \frac{(c_f C_f - c_r C_r)}{mv_x^2}), a_{21} = \frac{(c_r C_r - c_f C_f)}{I}, a_{22} = -\frac{(c_f^2 C_f + c_r^2 C_r)}{v_x I}, b_0 = \frac{C_f}{mv_x}, b_1 = \frac{c_f C_f}{I}$.

Substituting v_y in (3) by $v_x\beta$ gives

$$\dot{d} = v_x\beta + v_x e + d_0 \tag{8}$$

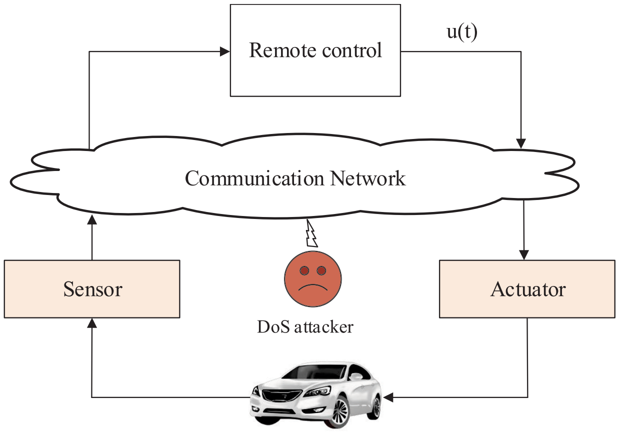


Fig. 3. Network control structure of AVs.

Combining (2), (7) and (8), the dynamics of the path following of AVs is written as

$$\begin{cases} \dot{d} = v_x\beta + v_x e + d_0 \\ \dot{e} = r - \rho(\sigma)v_x \\ \dot{\beta} = a_{11}\beta + a_{12}r + b_0\delta_f + d_1 \\ \dot{r} = a_{21}\beta + a_{22}r + b_1\delta_f + d_2 \end{cases} \tag{9}$$

Define the state vector $x(t) = [d, e, \beta, r]^T \in \mathbb{R}^{4\times 1}$, the control input $u(t) = \delta_f \in \mathbb{R}$ and the disturbance input vector $d(t) = [d_0, -\rho(\sigma)v_x, d_1, d_2]^T$ with an aggressive form $Fw(t)$, $w(t) \in [0, +\infty) \in \mathbb{R}$. The state-space form of the considered AVs can be given as follows:

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + Fw(t) \\ x(t_0) = x_0 \end{cases} \tag{10}$$

Therefore,

$$A = \begin{bmatrix} 0 & v_x & v_x & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & a_{11} & a_{12} \\ 0 & 0 & a_{21} & a_{22} \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ b_0 \\ b_1 \end{bmatrix}, \quad F = \begin{bmatrix} f(d_0) \\ f(\rho, v_x) \\ f(d_1) \\ f(d_2) \end{bmatrix}$$

with $f(\cdot)$is related to $\cdot$.

Autonomous vehicles communicate through a remote communication network, allowing the vehicles to exchange data with each other. The networked path-following control framework is shown in Fig. 3, from which it can be seen that the autonomous vehicles sensor measurements and feedback control signals are transmitted over unreliable communications networks that are subject to DoS attacks.

C. DoS Attacks Model

It is worth pointing out that the study of distributed DoS (DDoS) attack and coordinated defense requires knowledge regarding the interactive characteristics of control devices, communication network, and the physical environment [31], which is a difficult problem to handle and is thus left for our future work. In addition, there are two main methods for modeling DoS attacks in networked control systems/cyber-physical systems which are: Queueing model and Stochastic model, in which the queuing model for the analysis and study of the DoS attack on the networked control systems/cyber-physical systems has been widely used in the existing works. The queuing model considers a sequence of DoS off/on transitions and the time interval of the DoS attack during which no communication is available [32]. Let $T_{0,n} \triangleq \left[t_n, t_n + S_{off,n}\right), (n \in \mathbb{N}, t_n \geq 0)$ represent the nth sleeping interval of DoS attacks when communication is allowed and the attack signal is inactive, and $T_{1,n} \triangleq \left[t_n + S_{off,n}, t_{n+1}\right), n \in \mathbb{N}$ represents the nth active interval of DoS attacks in which the attack signal is active and the data packet cannot be transmitted. $S_{off,n}$ and $A_{on,n}$ represent the sleeping and active periods of the nth DoS attack. This means that for $n \in \mathbb{N}$, the nth attack signal starts at time $t_n + S_{off,n}$ and ends at time t_{n+1}. It should be noted that in this paper, the attack signal is aperiodic, which means that each sleep length $S_{off,n}$, is different. We assume that the control input signal on the wireless communication channel faces the aperiodic DoS attack signal represented by $\partial_{DoS}(t)(t \geq 0)$ denoted by

$$\partial_{DoS}(t) = \begin{cases} 0, & t \in T_{0,n} \\ 1, & t \in T_{1,n} \end{cases}$$

Clearly, if $S_{off,n}$ $A_{on,n}$ is arbitrarily chosen, the closed-loop system may be unstable, and the control objectives may not be achieved. Motivated by [33], it is necessary to make the following assumption:

Assumption 1: Both the sleep and active periods of the above DoS attack signal are lower and upper bounded, i.e., there exist four positive scalars $S_{off}^{\max}$, $S_{off}^{\min}$, $A_{on}^{\max}$ and $A_{on}^{\min}$ satisfying $S_{off}^{\min} \leq S_{off,n} \leq S_{off}^{\max}$ and $A_{on}^{\min} \leq A_{on,n} \leq A_{on}^{\max}$, where $A_{on,n} = t_{n+1} - (t_n + S_{off,n}) = A_n - S_{off,n}, A_n = t_{n+1} - t_n, n \in \mathbb{N}$.

Remark 1: The existing studies on DoS attacks have relatively strong assumptions, that is, DoS attacks have a certain statistical distribution [34], or dwell-time [25], [35], [36] or fixed period [33], [37], [38]. However, in practice, DoS attacks do not follow any given information, so the countermeasures can only be designed with limited and accessible information from the DoS attackers. In fact, adopting the identification method proposed in [33], the above four DoS attack parameters can be identified. Therefore, the above assumption is reasonable.

Remark 2: In most practical scenarios, data communication is allowed to continue after the DoS attack stops, causing the associated DoS attack to be in an intermittent active and sleeping period. Furthermore, the duration of each DoS attack is usually not too long due to the limited energy budget of the adversary. Therefore, $S_{off,n} \to 0$ and $A_{on,n} \to \infty$ do not occur. That is, one has $S_{off,n} > 0$ and $A_{on,n} < \infty$. On the other hand, if the sleep period is infinite, there is no attack, which is not the focus of the present paper. Therefore, $S_{off,n} < \infty$ and $A_{on,n} > 0$. Note that only three parameters $T_{off}^{\min}$, $T_{off}^{\max}$ and $T_{on}^{\max}$ are explored in [36] to address a resilient filter design problem, which may introduce a certain degree of design conservatism due to the lack of information on the lower bound $T_{on}^{\min}$ of $T_{on,n}$.

Remark 3: In fact, according to Assumption 1, we can estimate an upper bound on the average frequency of DoS off/on transitions by $\frac{1}{F_D} \approx \frac{1}{\varepsilon_{00}+\varepsilon_{10}}$ and an upper bound on the average duration of DoS per unit time by $\frac{1}{\Gamma} \approx \frac{1}{\varepsilon_{10}}$. Based on this estimations, it can be concluded that for a given time interval $[t_0, t]$ and the number of attacks $N(t, t_0)$ in this time interval (the total DoS attack duration $T(t, t_0)$ can be calculated), there exists a positive scalar υ_1 such that $N(t, t_0) \leq \upsilon_1 + \frac{t-t_o}{F_D}$ is satisfied. Similarly, there also exists a positive scalar υ_2 satisfying $T(t, t_0) \leq \upsilon_2 + \frac{t-t_o}{\Gamma}$. This property indicates that the DoS frequency constraints are satisfied automatically in the proposed framework. Therefore, the assumption on DoS attack model in this paper is more general than the classic one considered in [16] and [35] to some extent.

Remark 4: From the view of time characteristic of DoS attack, the attack frequency of the DoS refers to the number of attacks in a certain period of time. In actual network layer, the intensity of the DoS can be interpreted as attack rate, which indicates the highest rate of attack flows [39], [40]. When attack intensity was over the upper of the tolerant traffic, network communication would be interrupted completely. In the study of secure/resilient control, we consider the attack intensity which is enough to break the closed-loop communication. Moreover, DoS attacks with limited energy is intermittent. Under the intermittent DoS attack, the considered networked control system is generally modeled as a switched system with an unstable subsystem mode. To analyze the influence of DoS on/off transition, attack frequency is introduced to quantify this switching feature. In summary, the attack frequency and intensity should be discussed in different layers, namely control system layer and network layer.

D. Closed-Loop System Modeling

Consider the effect of the DoS attacks, the control input (see Fig. 2) can be expressed as

$$u(t) = \begin{cases} Kx(t), & t \in T_{0,n} \\ 0, & t \in T_{1,n} \end{cases} \tag{11}$$

where $K \in \mathbb{R}^{1\times 4}$ is the control gain to be designed.

To improve the vehicles path-following performance, e and d should be as small as possible. In addition, to enhance the stability of the vehicle, the yaw velocity r and sideslip angle β of the vehicle should be better controlled. Therefore, similar to [29], the controlled output $z(t) = [d, e, \beta, r]^T$ is defined as $z(t) = Zx(t)$, where $Z = diag(I)$. Combining (10) and (11), the path following control system (10) can be rewritten as:

$$\begin{cases} \dot{x}(t) = \begin{cases} (A + BK)x(t) + Fw(t), & t \in T_{0,n} \\ Ax(t) + Fw(t), & t \in T_{1,n} \end{cases} \\ z(t) = Zx(t) \\ x(t_0) = x_0 \end{cases} \tag{12}$$

For easy of exposition, define

$$\hat{A}_i = \begin{cases} A + BK, & i = 0 \\ A, & i = 1 \end{cases}$$

Therefore, (12) can be described as:

$$\begin{cases} \dot{x}(t) = \begin{cases} \hat{A}_0 x(t) + Fw(t), & t \in T_{0,n} \\ \hat{A}_1 x(t) + Fw(t), & t \in T_{1,n} \end{cases} \\ z(t) = Zx(t) \\ x(t_0) = x_0 \end{cases} \tag{13}$$

Next, the definitions of exponential stability and L_2-gain and a technical lemma will be given in proving the main results.

Definition 1: System (13) with $w(t) = 0$ is said to be exponentially stable if there exist two positive scalars α and ζ such that for all $t \geq 0$ and all $x_0 \in \mathbb{R}^4$:

$$\|x(t)\| \leq \alpha \|x_0\| e^{-\zeta t}.$$

Definition 2: System (13) is said to be exponentially stable with a L_2-gain less than γ if for any DoS jamming attacks signal $\partial_{DoS}(t)$ satisfying Assumption 1, the following two conditions are satisfied:

1. The system (13) with $w(t) = 0$ is exponentially stable;
2. For any non-zero $w(t) \in L_2[0, \infty)$, there exist a positive scalar γ such that

$$\int_0^\infty z^T(t)z(t)dt \leq \gamma^2 \int_0^\infty w^T(t)w(t)dt.$$

Lemma 1 [41] For matrices Q, P, Γ, M_0, M_{ij}, and X_j with appropriate dimensions, $i, j = 0, 1$, if they satisfy the following inequalities:

$$\begin{bmatrix} \Gamma + PM_0Q + (PM_0Q)^T & ((M_{ij} - M_0)Q)^T + PX_j \\ * & -X_j^T - X_j \end{bmatrix} < 0,$$

then it holds that $\Gamma + PM_{ij}Q + (PM_{ij}Q)^T < 0$.

III. Main Results

A. Stability Analysis Under DoS Attacks

To insert the four DoS parameters shown in Assumption 1 into the stability criteria, a key step is to define several auxiliary functions related to these DoS attack parameters. Inspired by [42], for $t \geq 0$, define

$$\eta_{0j,n}(t) = \begin{cases} \dfrac{t - t_n}{\eta'_{00}}, & j = 0 \\ \dfrac{t_n + S_{off,n} - t}{\eta'_{00}}, & j = 1 \end{cases} \quad (t \in T_{0,n})$$

$$\eta_{1j,n}(t) = \begin{cases} \dfrac{t - (t_n + S_{off,n})}{\eta'_{10}}, & j = 0 \\ \dfrac{t_{n+1} - t}{\eta'_{10}}, & j = 1 \end{cases} \quad (t \in T_{1,n})$$

where $\eta'_{00} = S_{off,n}$, $\eta'_{10} = A_n - S_{off,n}$. It can be seen that $\sum_{j=0}^{1} \eta_{ij,n}(t) = 1, i = 0, 1$. For $i = 0, 1$, $n \in \mathbb{N}$, define $t_{i,n} = \left\{\begin{smallmatrix} t_n, i=0 \\ t_n + S_{off,n}, i=1 \end{smallmatrix}\right.$ and then substituting it into the above auxiliary function sequences, we have

$$\eta_{i0,n}(t_{i,n}) = \eta_{i1,n}(t^-_{1-i,n+i}) = 0$$
$$\eta_{i1,n}(t_{i,n}) = \eta_{i0,n}(t^-_{1-i,n+i}) = 1.$$

Before proceeding further, we define $\varepsilon_{00} = S^{\min}_{off}$, $\varepsilon_{01} = S^{\max}_{off}$, $\varepsilon_{10} = A^{\min}_{on}$, $\varepsilon_{11} = A^{\max}_{on}$.

Theorem 1: If for some prescribed positive scalars ω_0, ω_1, ε_{ik}, γ, and matrix K, if there exist some positive definite matrices L_{ij}, i, $j, k = 0, 1$, such that

$$\begin{bmatrix} \Lambda_{ijk} & L_{ij}F & Z^T \\ * & -\bar{\omega}\gamma^2 I & 0 \\ * & * & -I \end{bmatrix} < 0 \tag{14}$$

and

$$L_{i1} \leq \omega_{1-i} L_{1-i,0} \tag{15}$$

where $\bar{\omega} = \frac{\min\{\omega_0, \omega_1, 1\}}{\max\{\omega_0, \omega_1, 1\}}$, $\Lambda_{ijk} = \frac{\ln \omega_i}{\varepsilon_{ik}} L_{ij} + \frac{1}{\varepsilon_{ik}}(L_{i0} - L_{i1}) + L_{ij}\hat{A}_i + \hat{A}_i^T L_{ij}$. Then the system (13) is exponentially stable.

Proof: See the Appendix A. ■

Remark 5: The system (13) displays a closed-loop mode over the sleeping period $t \in T_{0,n}$ and active period $t \in T_{1,n}$ of the DoS attack. To quantitatively characterize the effects of an intermittent DoS attack in a unified framework, an auxiliary function related to switching time $\eta_{ij,n}(t)$ is inserted into the candidate piecewise time-varying Lyapunov function $V(t)$. In addition, different matrices L_{ij} are introduced into $V(t)$ to increase the degrees of freedom, which reduces the conservatism of the proposed control design method.

Remark 6: Note that $V(t)$ is an attack-dependent time-varying Lyapunov function, which has several notable features compared to the attack-independent time-invariant Lyapunov function used by some existing works. Along the trajectory of system (13), $V(t)$ contains the upper and lower bounds of the length of the DoS sleeping and DoS active periods. Therefore, this work uses more information on DoS attacks with the help of a time-varying Lyapunov function to reduce the design conservatism.

B. L_2-Gain Control Synthesis Under DoS Attacks

Theorem 2: If for some prescribed positive scalars ω_0, ω_1, ε_{ik}, λ_0, λ_1, and γ, there exist matrices M_0, $M_{ij} > 0$, and $\tilde{K}$ with appropriate dimensions, $i, j = 0, 1$, such that the following LMIs hold:

$$\begin{bmatrix} \Phi_{00k} & \varsigma^T(M_{00} - M_0^T + \lambda_0 B\tilde{K}) \\ * & -\lambda_0(M_0 + M_0^T) \end{bmatrix} < 0 \tag{16}$$

$$\begin{bmatrix} \Phi_{01k} & \varsigma^T M_{01} & \varsigma^T(M_{01} - M_0^T + \lambda_1 B\tilde{K}) \\ M_{01}\varsigma & -\varepsilon_{0k} M_{00} & 0 \\ * & * & -\lambda_1(M_0 + M_0^T) \end{bmatrix} < 0 \tag{17}$$

$$\Phi_{10k} < 0 \tag{18}$$

$$\begin{bmatrix} \Phi_{11k} & \varsigma^T M_{11} \\ M_{11}\varsigma & -\varepsilon_{1k} M_{10} \end{bmatrix} < 0 \tag{19}$$

$$M_{00} \leq \omega_0 M_{11}, \quad M_{10} \leq \omega_1 M_{01} \tag{20}$$

where $k = 0, 1$, and

$$\varsigma = \begin{bmatrix} I & 0 & 0 \end{bmatrix}$$

$$\Phi_{ijk} = \begin{bmatrix} \Pi_{ijk} & F & M_{ij}Z^T \\ * & -\bar{\omega}\gamma^2 I & 0 \\ * & * & -I \end{bmatrix}$$

with

$$
\begin{aligned}
\Pi_{00k} &= \frac{\ln\omega_0 + 1 - 2\tau_0}{\varepsilon_{0k}} M_{00} + \frac{\tau_0^2}{\varepsilon_{0k}} M_{01} + AM_{00} \\
&\quad + M_{00}^T A^T + B\tilde{K} + \tilde{K}^T B^T \\
\Pi_{01k} &= \frac{\ln\omega_0 - 1}{\varepsilon_{0k}} M_{01} + AM_{01} + M_{01}^T A^T + B\tilde{K} \\
&\quad + \tilde{K}^T B^T \\
\Pi_{10k} &= \frac{\ln\omega_1 + 1 - 2\tau_1}{\varepsilon_{1k}} M_{10} + \frac{\tau_1^2}{\varepsilon_{1k}} M_{11} + AM_{10} \\
&\quad + M_{10}^T A^T \\
\Pi_{11k} &= \frac{\ln\omega_1 - 1}{\varepsilon_{1k}} M_{11} + AM_{11} + M_{11}^T A^T
\end{aligned}
$$

Then, the system (13) is exponentially stabilized by the attack-resilient state-feedback controller (11) with $K = \tilde{K}M_0^{-1}$ and has a L_2-gain less than γ.

Proof: See the Appendix B. ■

Remark 7: Theorem 2 proposes a design method for the L_2-gain controller, which is expressed in the form of LMIs. From Theorem 2, the feasibility of the LMIs is related to the parameters ω_i, τ_i and λ_i, $i = 0, 1$. In general, the complexity of the LMI computations is polynomial time bounded by $O(RN^3 log(C/v))$, where R is the total row size of the LMIs, N is the number of scalar decision variables, C is the scaling factor and v is the relative accuracy set for the algorithm. Here, we assume that the system dimension is n and that the involved variable dimensions can be determined by M_0, M_{ij}, $i, j = 0, 1$. Then, for Theorem 2, $R = 18n$ and $N = 3n^2+3n$. Thus, the computational complexity of Theorem 2 can be expressed as $O(n^7)$, which polynomially depends on the size of the system. Therefore, the parameters ω_i, τ_i, λ_i, $i = 1, 2$ can be suitably chosen while guaranteeing the feasibility of the LMIs (16)-(20).

C. Algorithm

Based on Theorem 2, we first provide an Algorithm 1 to design control gain matrix K for system (13). The detailed procedures are shown in Algorithm 1 below.

Algorithm 1 The Design of Controller Gain Matrix K

```
Input: the system parameter matrices $A$, $B$ and $F$;
       positive scalars $\gamma$, $\tau_0$, $\tau_1$, $\omega_0$, $\omega_1$, $\lambda_0$, $\lambda_1$; the
       sleeping and attack parameters $\varepsilon_{00}$, $\varepsilon_{01}$, $\varepsilon_{10}$,
       $\varepsilon_{11}$.
Output: $K$
LMI toolbox in MATLAB is used to solve
  LMIs (16)-(20);
if $t_{min} \geq 0$ then
    go to Input to adjust positive scalars and the
      sleeping and attack parameters;
else
    solve $\tilde{K}$ and $M_0^{-1}$ with LMIs (16)-(20) and
      substitute them into $K = \tilde{K}M_0^{-1}$;
end
The state-feedback gain $K$ is obtained.
```

Then for the system (13) with a designed controller K, the minimal L_2-gain γ_{min} can be derived from the Theorem 2 by applying the common binary search technique. The corresponding algorithm is given below.

Algorithm 2 An Algorithm for Finding γ_{min}

```
Input: Input the system parameter matrices $A$, $B$, $F$;
       positive sclars $\tau_0$, $\tau_1$, $\omega_0$, $\omega_1$, $\lambda_0$; $\lambda_1$; set
       sufficiently small step increment e=0.0001 and
       a search interval $[\gamma_h, \gamma_z]$, where $\gamma_h = 0$ and
       appropriate value $\gamma_z$.
Output: $\gamma_{min}$
while $|\gamma_h - \gamma_z| > e$ do
    $\gamma_m = (\gamma_z - \gamma_h)/2$
    if LMIs (16)-(20) are feasible then
        $\gamma_z = \gamma_m$
    else
        $\gamma_h = \gamma_m$
    end
end
return $\gamma_{min} = \gamma_m$.
```

IV. Simulation Study

In this section, a series of numerical simulations are carried out to demonstrate the effectiveness of the proposed attack-resilient path following controller for autonomous vehicles proposed in [29]. The parameters of the vehicle model shown in (10) are given by

$$
A = \begin{bmatrix} 0 & 25 & 25 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -0.853 & -0.996 \\ 0 & 0 & 1.6 & -2.336 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ 1.067 \\ 20.8 \end{bmatrix},
$$

$$
F = \begin{bmatrix} 0.350 & 0.105 & 0.095 & 0.096 \end{bmatrix}^T.
$$

A. Design of L_2-Gain-Based Path Following Controller

First, we discuss the design of a state feedback-based path following controller for the considered autonomous vehicle under DoS attacks and external disturbance. For this purpose, the DoS attack parameters are chosen as $\varepsilon_{00} = 0.6, \varepsilon_{01} = 1.2, \varepsilon_{10} = 0.5, \varepsilon_{11} = 1.0$, the prescribed L_2-gain $\gamma = 100$, the other tuning parameters $\omega_0 = 2, \omega_1 = 2, \tau_0 = 1.35, \tau_1 = 3.0, \lambda_0 = 0.3, \lambda_1 = 0.3$. The sampling period $h = 0.1s$. Then, by solving LMIs (16)-(20) in Theorem 2, the attack-resilient state-feedback path following controller gain K is given by

$$
K = \begin{bmatrix} -0.0244 & -1.1208 & -0.6700 & -0.1258 \end{bmatrix}
$$

Next, we study the stability of the attacked autonomous vehicle with $w(t) = 0$ under the above attack-resilient path following controller. To this end, set the initial state $x_0 = \begin{bmatrix} 3 & 0 & 1 & -5 \end{bmatrix}^T$. The number of DoS attacks is set to be 15. The attack instants are generated randomly. Fig. 4 and Fig. 5 show the state responses of the system without/with DoS attacks, respectively. By comparing Fig. 4 and Fig. 5, it can be seen that the system no longer floats up and down when it

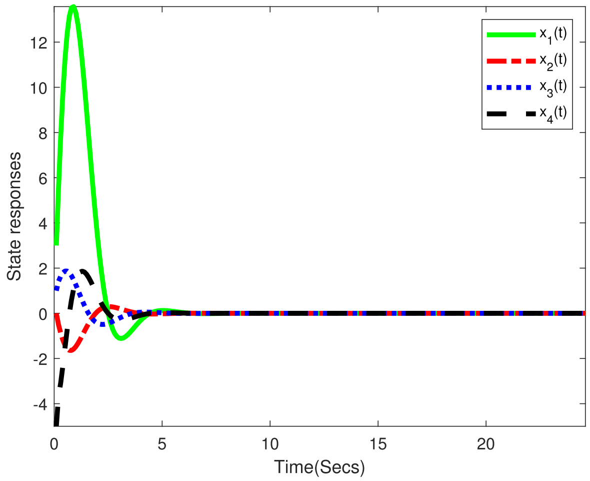


Fig. 4. State responses without DoS attacks.

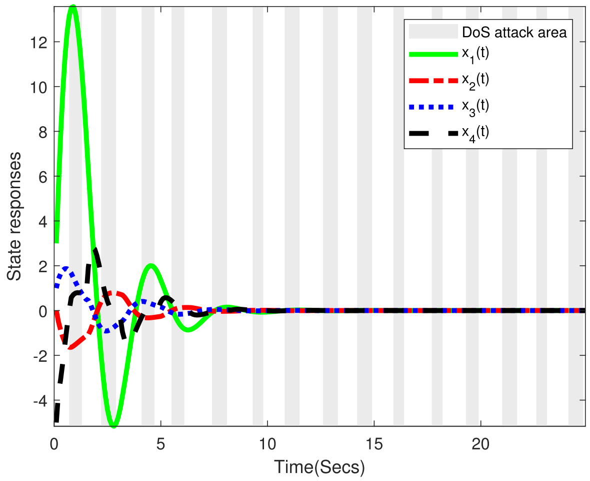


Fig. 5. State responses with $w(t) = 0$.

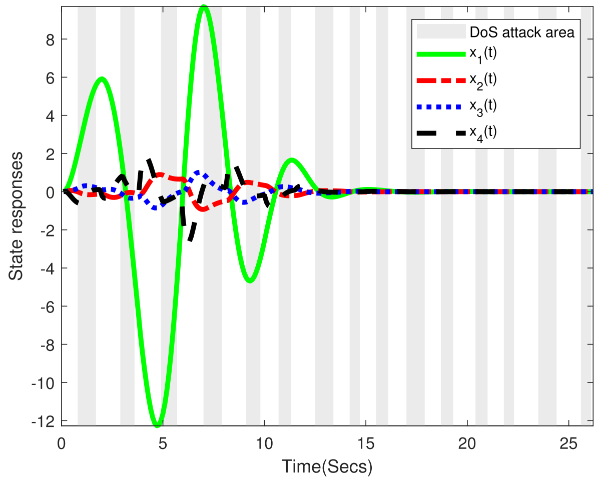


Fig. 6. State responses in the presence of $w(t)$.

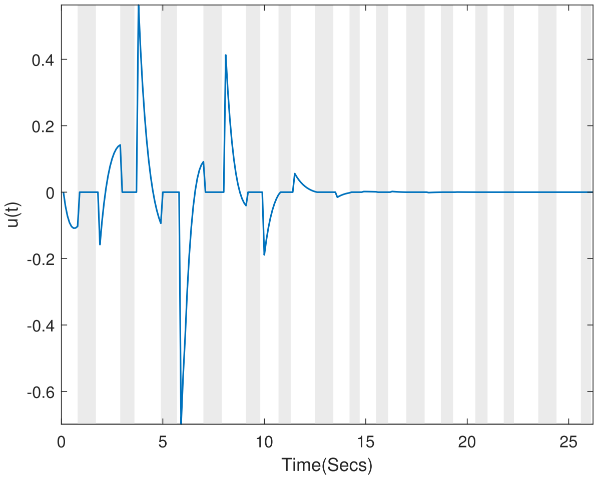


Fig. 7. The control input under DoS attacks.

TABLE I

THE MINIMUM VALUES OF γ FOR DIFFERENT ε_{01}

ε_{00}	0.6	0.6	0.6	0.6
ε_{01}	0.8	1.0	1.2	1.4
$\gamma_{\min}$	22.9831	21.9861	19.9885	16.9951

TABLE II

THE MINIMUM VALUES OF γ FOR DIFFERENT ε_{11}

ε_{10}	0.5	0.5	0.5	0.5
ε_{11}	1.0	0.8	0.7	0.6
$\gamma_{\min}$	19.9885	19.9501	13.6760	11.8401

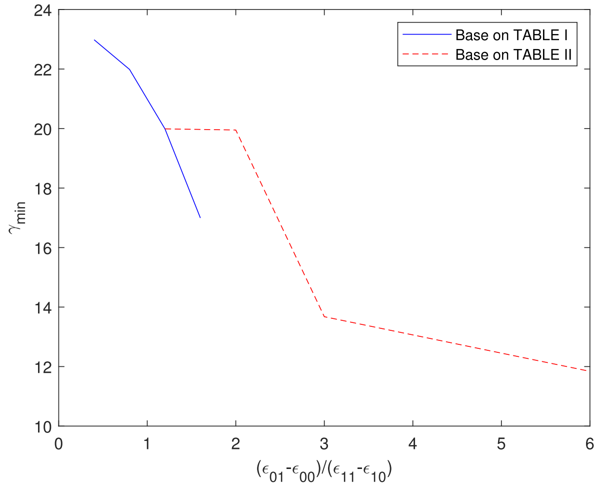
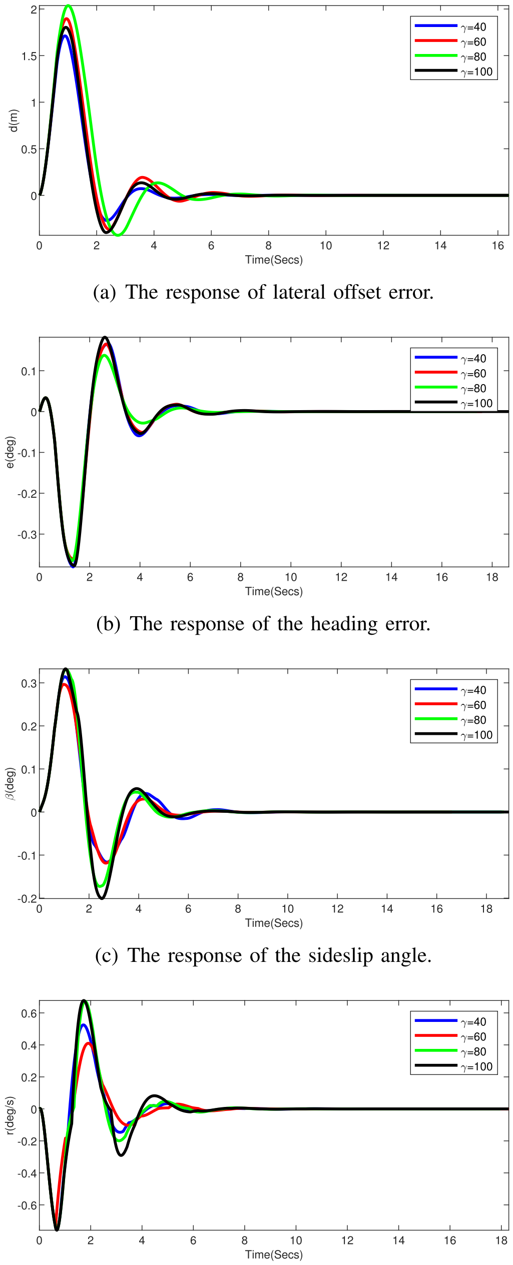


Fig. 8. $\gamma_{\min}$ obtained with different values of $(\varepsilon_{01} - \varepsilon_{00})/(\varepsilon_{11} - \varepsilon_{10})$.

is stable without DoS attacks, while the system wobbles and vibrates up and down until it is stabilized when DoS attacks exist, which validates the attacked system is still stable despite the presence of the DoS attacks. Furthermore, we evaluate the joint effect of DoS attacks and external disturbance on the closed-loop system. We assume the external disturbance $w(t) = 2\cos(t)$ when $0s \leq t \leq 6s$, otherwise, $w(t) = 0$. The state responses of the system and control input under DoS attacks are depicted in Fig. 6 and Fig. 7, respectively. In addition, under the above given parameters, we obtain the achieved minimum value of L_2-gain $\gamma^* = 2.2202 < 100$, which proves the effectiveness of our proposed method.



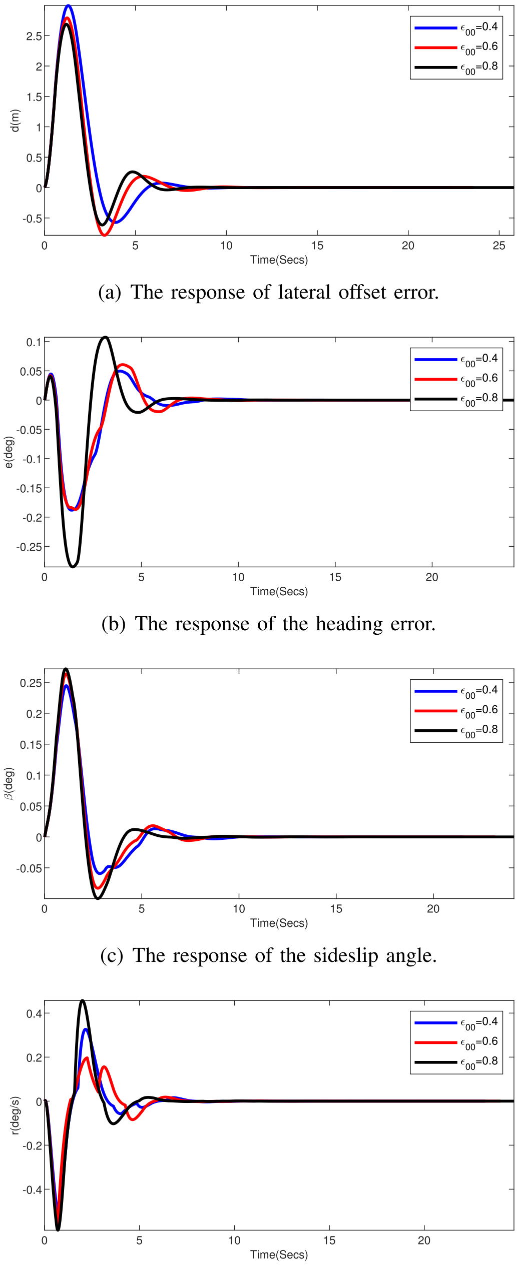
(a) The response of lateral offset error.

(b) The response of the heading error.

(c) The response of the sideslip angle.

(d) The response of the yaw rate.

Fig. 9. The state responses of vehicle under different values of γ.



(a) The response of lateral offset error.

(b) The response of the heading error.

(c) The response of the sideslip angle.

(d) The response of the yaw rate.

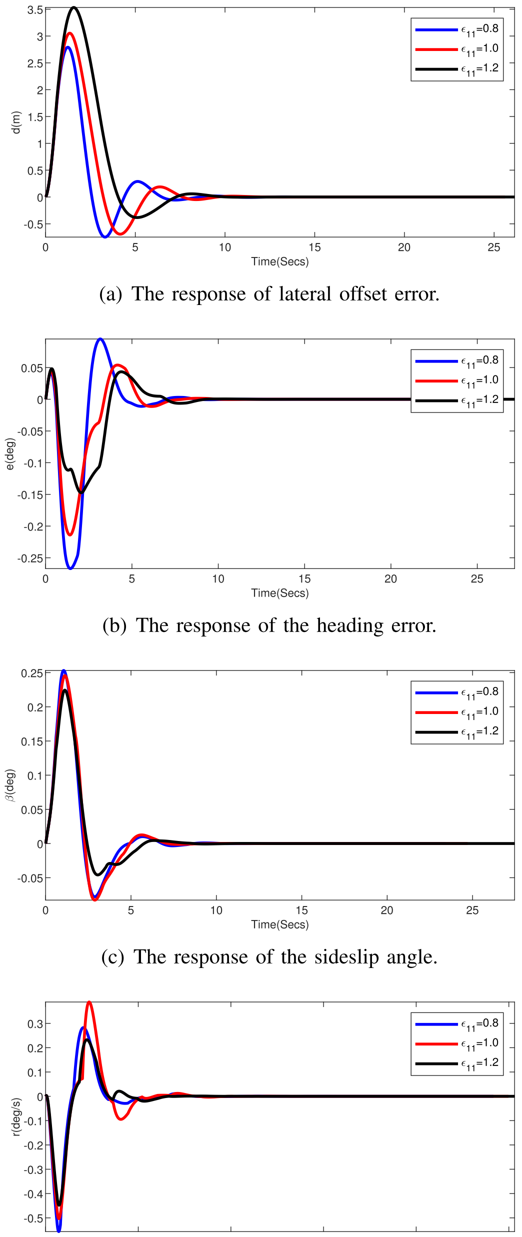
Fig. 10. The state responses of vehicle under different values of ε_{00}.

B. The Impact of DoS Attack Parameters on the L_2-Gain λ

TABLE I shows the impact of different values of ε_{01} on the minimum values of $\gamma_{\min}$ for fixed $\varepsilon_{00} = 0.6$, $\varepsilon_{10} = 0.5$, and $\varepsilon_{11} = 1.0$. As shown in TABLE I, it can be observed that $\gamma_{\min}$ decreases as ε_{01} increases, with the other parameters are fixed. Further, set $\varepsilon_{00} = 0.6$ and $\varepsilon_{01} = 1.2$. For different values of ε_{11}, the obtained minimum values of $\gamma_{\min}$ are listed in TABLE II. From TABLE II, we can observe that $\gamma_{\min}$ decreases as ε_{11} decreases. Based on the above computation results, it can be concluded that the upper and lower bounds of the sleeping time and active time of the DoS attacks do have an impact on the L_2-gain performance of the considered system. To clearly show this tendency, we plot the Fig. 8 on the basis of the Tables I and II. As shown in Fig. 8, a larger $(\varepsilon_{01} - \varepsilon_{00})/(\varepsilon_{11} - \varepsilon_{10})$ leads to a smaller γ, leading to better system performance. According to the definition of DoS attacks, it is seem that as the ratio of $S_{off,n}$ to $A_{on,n}$ increases, the systems anti-attack ability becomes increasingly stronger.

C. The Comparison of State Responses Under Different L_2-Gain and DoS Attack Parameters

To further explore the influence of DoS attacks on the state responses of the autonomous vehicle with the proposed path-following control method in more detail, in the following simulation, the external disturbance $w(t) = 2\cos(t)$ is selected when $0s \leq t \leq 0.6s$, otherwise, $w(t) = 0$. The sampling period $h = 0.01s$. For given different values of γ, ε_{00},



(a) The response of lateral offset error.

(b) The response of the heading error.

(c) The response of the sideslip angle.

(d) The response of the yaw rate.

Fig. 11. The state responses of vehicle under different values of ε_{11}.

and ε_{11}, the corresponding state responses are shown in Figs. 9-11, respectively. Specifically, Fig. 9 shows the respective state responses for $\gamma = 40, 60, 80, 100$, respectively, while the other parameters remain unchanged. It is worth pointing out that when taking different DoS parameters in the simulations, the state responses of the AVs change correspondingly.

Fig. 10 and Fig. 11 show the corresponding state responses when the attack parameters ε_{00} and ε_{11} are changed, respectively. In these cases, the prescribed L_2-gain $\gamma = 100$. For given $\varepsilon_{00} = 0.4, 0.6$ and 0.8, it can be seen from Fig. 10 that, with the increase of ε_{00}, the convergence time becomes shorter. This indicates that the longer the sleeping period of the DoS attacker is, the less influence it has on the vehicle path following control performance. Similarly, for given $\varepsilon_{11} = 0.8, 1.0, 1.2$, it can be observed from Fig. 11 that, the convergence time is shortest when $\varepsilon_{11} = 0.8$. This also indicates that the shorter the active time period of the DoS attacker is, the better the system performance.

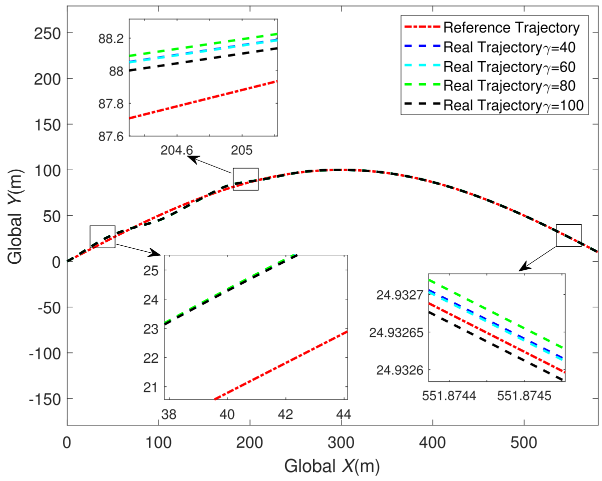


Fig. 12. The comparison between the desired and actual paths of the attacked vehicle.

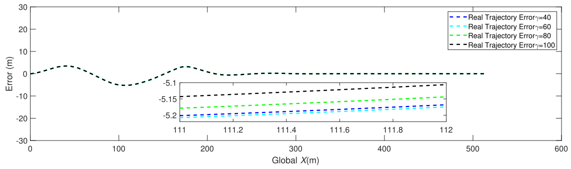


Fig. 13. Deviation error between actual paths and desired path.

D. The Comparison of Path Following Under Different L_2-Gains

To further compare the desired and actual paths of the attacked vehicle under different L_2 performances, we show the path following results in Fig. 12 with $\varepsilon_{00} = 0.6$, $\varepsilon_{01} = 1.2, \varepsilon_{10} = 0.2, \varepsilon_{11} = 0.4, \omega_0 = 2, \omega_1 = 2, \tau_0 = 1.35, \tau_1 = 3.0, \lambda_0 = 0.3, \lambda_1 = 0.3$. The sampling period $h = 0.01s$. The external disturbance is chosen as before. It can be seen from Fig. 12 that the path tracking effect seems normal despite the simultaneous presences of the intermittent DoS attacks and external disturbances. Furthermore, in order to clearly show the deviations between actual path and desired path, we have added a new deviation error shown in Fig.13, from which it can be seen that there exist some deviation errors between the actual path of the AV and the desired path. This is because the overshoot of the AV is large at first (see Fig. 6), which is caused by external disturbance and DoS attacks. Fortunately, the deviation error converges to around equilibrium point 0 gradually as the states of the AV approach to equilibrium point 0 under the proposed path following control strategy.

Overall, the above simulation results confirm that the effectiveness of the proposed attack-resilient path following control for autonomous vehicles under DoS attacks and external interference.

V. Conclusion

In this paper, a resilient path-following controller has been proposed for autonomous vehicles under a new type of aperiodic DoS attacks. Attack parameter-dependent time varying Lyapunov function approach has been employed to analyze the stability and L_2-gain of the resulting autonomous vehicles. The attack parameter-dependent sufficient conditions for exponential stability and L_2-gain have been derived in terms of LMIs. The path-following controller gain can be obtained by solving a set of LMIs. Finally, the applicability of the proposed resilient path-following controller has been validated by simulation results. To develop a resilient path-following controller by considering coordinated DoS attacks and sensor/actuator FDI attacks for autonomous vehicles will be addressed in the future work. Furthermore, the derived main results largely rely on the linear time-invariant state-space model (10) of the AVs. To enable practical applicability, it thus would be interesting to loose the requirement of an accurate AVs model and further devise effective and resilient path following control approaches against hybrid attacks.

Appendix A
Proof of Theorem 1

First, we establish the exponential stability of the closed-loop control system (13) under the condition of Theorem 1. To this end, suppose $w(t) = 0$, then the system (13) can be rewritten as

$$\begin{cases} \dot{x}(t) = \hat{A}_i x(t), t \in T_{i,n} \\ x(t_0) = x_0 \end{cases} \tag{21}$$

From (14), we can conclude that there exists a sufficiently small positive scalar ζ satisfying

$$\tilde{\Lambda}_{ijk} < 0, , i, j, k = 0, 1 \tag{22}$$

where $\tilde{\Lambda}_{ijk} = (\frac{\ln \omega_i}{\varepsilon_{ik}} + \zeta)L_{ij} + \frac{1}{\varepsilon_{ik}}(L_{i0} - L_{i1}) + L_{ij}\hat{A}_i + \hat{A}_i^T L_{ij}$.

Choose the following candidate Lyapunov function for the system (21):

$$V(t) = \delta(t)x^T(t)\sum_{j=0}^{1}\eta_{ij,n}(t)L_{ij}x(t)$$

where $\delta(t) = \omega_i^{\eta_{i0,n}(t)}$

For any given initial value $x_0 \in \mathbb{R}^{n_1}$, set $x(t) = x(t, 0, x_0)$, and $W(t) = e^{\zeta t}V(t)$. For $t \in (t_{i,n}, t_{1-i,n+i})$ with any fixed $i \in \{0, 1\}$ and $n \in \mathbb{N}$, the time derivative of $W(t)$ along the solutions system (21) is

$$\dot{W}(t) = e^{\zeta t}\delta(t)\sum_{j=0}^{1}\eta_{ij,n}(t)x^T(t)[(\frac{\ln \omega_i}{\eta'_{i0}} + \zeta)L_{ij} + \frac{1}{\eta'_{i0}}(L_{i0} - L_{i1}) + L_{ij}\hat{A}_i + \hat{A}_i^T L_{ij}]x(t) \tag{23}$$

Therefore, we can obtain

$$\begin{aligned} \dot{W}(t) &\leq e^{\zeta t}\delta(t)\sum_{j=0}^{1}\eta_{ij,n}(t)x^T(t)\tilde{\Lambda}_{ijk}x(t) \\ &< 0 \end{aligned}$$

Then it follows that

$$V(t) \leq V(t_{i,n})e^{-\zeta(t - t_{i,n})}, t \in \left(t_{i,n}, t_{1-i,n+i}\right) \tag{24}$$

From (15), it follows that

$$\begin{aligned} V(t_{i,n}) &= \delta(t_{i,n})x^T(t_{i,n})\sum_{j=0}^{1}\eta_{ij,n}(t_{i,n})L_{ij}x(t_{i,n}) \\ &= x^T(t_{i,n})L_{i1}x(t_{i,n}) \\ &\leq \omega_{1-i}x^T(t_{i,n})L_{1-i,1}x(t_{i,n}) \\ &= V(t_{i,n}^-) \end{aligned} \tag{25}$$

Combing (24) and (25), we have

$$V(t) \leq V(0)e^{-\zeta t}$$

Notice that

$$\begin{aligned} \delta(t)\left\|x(t)\right\|^2\phi_1 &\leq \delta(t)x^T(t)\sum_{j=0}^{1}\eta_{ij,n}(t)L_{ij}x(t) \\ &\leq \omega_0^{\eta_{00,n}(0)}x^T(0)\sum_{j=0}^{1}\eta_{0j,n}(0)L_{0j}x(0)e^{-\zeta t} \\ &\leq \phi_2\left\|x(0)\right\|^2 e^{-\zeta t} \end{aligned}$$

which implies that

$$\|x(t)\| \leq e^{-\frac{\zeta}{2}t}\sqrt{\frac{\phi_2}{\phi_1\delta(t)}}\|x(0)\|$$

where $\phi_1 = \lambda_{\min}(L_{ij})$, $\phi_2 = \lambda_{\max}(L_{i1})$, $i, j = 0, 1$. Because $\eta_{i0,n}(t) < 1$, it is easy to see that $\delta(t) = \omega_i^{\eta_{i0,n}(t)} \geq \min\{\omega_0, \omega_1, 1\}$. Therefore, the above inequality can be further rewritten as

$$\|x(t)\| \leq e^{-\frac{\zeta}{2}t}\sqrt{\frac{\phi_2}{\phi_1 \min\{\omega_0, \omega_1, 1\}}}\|x(0)\|$$

According to Definition 1, the system (13) is exponentially stable under the time-constrainted DoS attacks.

Next, we shall prove that under the zero initial condition, the output $z(t)$ satisfies the relation shown in Definition 2. To this end, we introduce a function

$$F(t) = \int_0^t \delta(s)(z^T(s)z(s) - \bar{\omega}\gamma^2 w^T(s)w(s))ds, t \geq 0$$

For any $t \geq 0$, there exist a n such that $t \in T_{0,n}$ or $t \in T_{1,n}$. Without loss of generality, we assume $t \in T_{0,n}$. Then, combining $V(t_{0,n}) = 0$ and (25), one has

$$\begin{aligned} \int_0^t \dot{V}(s)ds &= \sum_{n=0}^{r-1}\left(\int_{t_{0,n}}^{t_{1,n}}\dot{V}(s)ds + \int_{t_{1,n}}^{t_{0,(n+1)}}\dot{V}(s)ds\right) \\ &\quad + \int_{t_{0,r}}^{t}\dot{V}(s)ds \\ &= \sum_{n=0}^{r-1}[V(t_{1,n}^-) - V(t_{0,n}) + V(t_{0,(n+1)}^-) \\ &\quad - V(t_{1,n})] + V(t) - V(t_{0,r}) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{n=0}^{r-1}[V(t_{1,n}^{-}) - V(t_{1,n})] + \sum_{n=0}^{r}[V(t_{0,n}^{-}) \\
&\quad - V(t_{0,n})] + V(t) \\
&\geq 0
\end{aligned}
$$

which implies

$$
F(t) \leq \int_0^t \Big(\delta(s)(z^T(s)z(s) - \bar{\omega}\gamma^2 w^T(s)w(s)) + \dot{V}(s)\Big)\, ds
$$

For any $s \in (t_{i,n}, t_{1-i,n+i})$ with any fixed $i \in \{0,1\}$ and $n \in \mathbb{N}$, along the solution of system (13), we obtain

$$
\begin{aligned}
&(\delta(s)(z^T(s)z(s) - \bar{\omega}\gamma^2 w^T(s)w(s)) + \dot{V}(s) \\
&= \delta(s)\sum_{j=0}^{1}\eta_{ij,n}(s)x^T(s)[\frac{\ln\omega_i}{\eta^{'}_{i0}}L_{ij} + \frac{1}{\eta^{'}_{i0}}(L_{i0} - L_{i1}) \\
&\quad + L_{ij}\hat{A}_i + \hat{A}_i^T L_{ij}]x(t) + \delta(s)(\sum_{j=0}^{1}\eta_{ij,n}(t)z^T(s)z(s) \\
&\quad - \bar{\omega}\gamma^2 w^T(s)w(s)) \\
&\leq \delta(s)\sum_{j=0}^{1}\eta_{ij,n}(s)v^T(s)(\Xi_{ijk} + G^T G)v(s)
\end{aligned}
$$

where $v(s) = \begin{bmatrix} x^T(s) & w^T(s) \end{bmatrix}^T$, $G = [\, Z \quad 0\,]$, and

$$
\Xi_{ijk} = \begin{bmatrix} \Lambda_{ijk} & L_{ij}F \\ * & \bar{\omega}\gamma^2 I \end{bmatrix}
$$

Applying Schur complement to LMIs (14) leads to $\Xi_{ijk} + G^T G < 0$. Thus, it follows that

$$
(\delta(s)(z^T(s)z(s) - \bar{\omega}\gamma^2 w^T(s)w(s)) + \dot{V}(s) < 0
$$

which is equivalent to

$$
\int_0^t \delta(s)z^T(s)z(s) \leq \bar{\omega}\gamma^2 \int_0^t w^T(s)w(s))ds
$$

where we have used the fact that $\min\{\omega_0, \omega_1, 1\} \leq \delta(s) \leq \max\{\omega_0, \omega_1, 1\}$. According to Definition 2 and noting the arbitrary of t, the proof is complete.

Appendix B
Proof of Theorem 2

Define $M_{ij} = L_{ij}^{-1}$, $K = \tilde{K}M_0^{-1}$,$i, j = 0, 1$. First discuss $i = j = 0$. Pre-and post-multiplying (14) by $\begin{bmatrix} M_{00} & 0 & 0 \\ 0 & I & 0 \\ 0 & 0 & I \end{bmatrix}$ yields that

$$
\Sigma_{00k} = \begin{bmatrix} \Omega_{00k} & F & M_{00}Z^T \\ * & -\bar{\omega}\gamma^2 I & 0 \\ * & * & -I \end{bmatrix} < 0
$$

in which

$$
\begin{aligned}
\Omega_{00k} = \frac{\ln\omega_0}{\varepsilon_{0k}}M_{00} + \frac{1}{\varepsilon_{0k}}M_{00}(L_{00} - L_{01})M_{00} \\
+ \hat{A}_0 M_{00} + M_{00}\hat{A}_0^T
\end{aligned}
$$

Σ_{00k} can be written as $\Sigma_{00k} = \hat{\Sigma}_{00k} + N_{00}$, where

$$
N_{00} = \begin{bmatrix} n_{00} & 0 & 0 \\ * & 0 & 0 \\ * & * & 0 \end{bmatrix}
$$

in which $n_{00} = BKM_{00} + M_{00}K^T B^T - BKM_0 - M_0^T K^T B^T$, and

$$
\hat{\Sigma}_{00k} = \begin{bmatrix} \hat{\Omega}_{00k} & F & M_{00}Z^T \\ * & -\bar{\omega}\gamma^2 I & 0 \\ * & * & -I \end{bmatrix} < 0 \tag{26}
$$

in which

$$
\begin{aligned}
\hat{\Omega}_{00k} = \frac{\ln\omega_0}{\varepsilon_{0k}}M_{00} + \frac{1}{\varepsilon_{0k}}M_{00}(L_{00} - L_{01})M_{00} + AM_{00} \\
+ M_{00}A^T + BKM_0 + M_0^T K^T B^T
\end{aligned}
$$

Using Schur complement and the matrix inequalities:

$$
-M_{00}M_{01}^{-1}M_{00} \leq \tau_0^2 M_{01} - 2\tau_0 M_{00}
$$

we obtain

$$
\begin{aligned}
\hat{\Omega}_{00k} &= \frac{\ln\omega_0}{\varepsilon_{0k}}M_{00} + \frac{1}{\varepsilon_{0k}}M_{00}(L_{00} - L_{01})M_{00} + AM_{00} \\
&\quad + M_{00}A^T + BKM_0 + M_0^T K^T B^T \\
&\leq \frac{\ln\omega_0 + 1}{\varepsilon_{0k}}M_{00} + \frac{1}{\varepsilon_{0k}}(-\tau_0 M_{00} + \tau_0^2 M_{01}) \\
&\quad + AM_{00} + M_{00}A^T + BKM_0 + M_0^T K^T B^T \\
&= \frac{\ln\omega_0 + 1 - 2\tau_0}{\varepsilon_{0k}}M_{00} + \frac{\tau_0^2}{\varepsilon_{0k}}M_{01} + AM_{00} + M_{00}A^T \\
&\quad + B\tilde{K} + \tilde{K}^T B^T \\
&= \Pi_{00k}
\end{aligned}
$$

By using Shur complement, (26) can be written as Φ_{00k}. And we can also prove that $\hat{\Sigma}_{01k} = \begin{bmatrix} \hat{\Omega}_{01k} & F & M_{01}Z^T \\ * & -\bar{\omega}\gamma^2 I & 0 \\ * & * & -I \end{bmatrix}$ can be rewritten as $\begin{bmatrix} \Phi_{01k} & \varsigma^T M_{01} \\ M_{01}\varsigma & -\varepsilon_{0k}M_{00} \end{bmatrix}$.

It is easy to see that the matrix inequalities (20) are equivalent to (15). From (16)-(17), we obtain that

$$
\begin{bmatrix} \bar{\Sigma}_{0jk} + PM_0Q + (PM_0Q)^T & Z \\ * & -\lambda_j M_0^T - \lambda_j M_0 \end{bmatrix} < 0 \tag{27}
$$

where $Q = \begin{bmatrix} I & 0 & 0 \end{bmatrix}$, $P = \begin{bmatrix} K^T B^T & 0 & 0 \end{bmatrix}^T$, $Z = ((M_{0j} - M_0)Q)^T + P(\lambda_j M_0)$ and

$$
\bar{\Sigma}_{0jk} = \begin{bmatrix} \bar{\Omega}_{0jk} & F & M_{0j}Z^T \\ * & -\bar{\omega}\gamma^2 I & 0 \\ * & * & -I \end{bmatrix}
$$

in which

$$
\begin{aligned}
\bar{\Omega}_{0jk} = \frac{\ln\omega_0}{\varepsilon_{0k}}M_{0j} + \frac{1}{\varepsilon_{0k}}M_{0j}(L_{00} - L_{01})M_{0j} \\
+ AM_{0j} + M_{0j}^T A^T
\end{aligned}
$$

In the light of Lemma 1, the matrix inequalities (27) imply that

$$\bar{\Sigma}_{0jk} + PM_{0j}Q + (PM_{0j}Q)^T < 0,\ j,k = 0,1 \tag{28}$$

Pre-and post-multiplying (28) by $diag(P_{0j}, I, I)$ yields that the matrix inequalities (29) are equivalent to (14) with $i = 0$. Using the similar technique, it is easy to show that the matrix inequalities (18)-(19) imply (14) with $i = 1$. This completes the proof.

References

[1] U. E. Larson and D. K. Nilsson, "Securing vehicles against cyber attacks," in *Proc. 4th Annu. Workshop Cyber Secur. Inf. Intell. Res. Developing Strategies Meet Cyber Secur. Inf. Intell. Challenges Ahead*, May 2008, pp. 1–3.

[2] J. Ni, J. Hu, and C. Xiang, "Robust control in diagonal move steer mode and experiment on an X-by-wire UGV," *IEEE/ASME Trans. Mechatronics*, vol. 24, no. 2, pp. 572–584, Apr. 2019.

[3] A. Palanca, E. Evenchick, F. Maggi, and S. Zanero, "A stealth, selective, link-layer denial-of-service attack against automotive networks," in *Proc. Int. Conf. Detect. Intrus. Malware Vulnerabil. Assessment*, 2017, pp. 185–206.

[4] M. C. Chow, M. Ma, and Z. Pan, "Attack models and countermeasures for autonomous vehicles," *Intelligent Technologies Internet Vehicles*. Cham, Switzerland: Springer, 2021, pp. 375–401.

[5] M. A. Zakaria, H. Zamzuri, R. Mamat, and S. A. Mazlan, "A path tracking algorithm using future prediction control with spike detection for an autonomous vehicle robot," *Int. J. Adv. Robotic Syst.*, vol. 10, no. 8, p. 309, Aug. 2013.

[6] J. C. McCall and M. M. Trivedi, "Driver behavior and situation aware brake assistance for intelligent vehicles," *Proc. IEEE*, vol. 95, no. 2, pp. 374–387, Feb. 2007.

[7] P. Zhao, J. Chen, T. Mei, and H. Liang, "Dynamic motion planning for autonomous vehicle in unknown environments," in *Proc. IEEE Intell. Vehicles Symp.*, Jun. 2011, pp. 284–289.

[8] M. S. Netto, S. Chaib, and S. Mammar, "Lateral adaptive control for vehicle lane keeping," in *Proc. Amer. Control Conf.*, vol. 3, 2004, pp. 2693–2698.

[9] S. Hima, S. Glaser, A. Chaibet, and B. Vanholme, "Controller design for trajectory tracking of autonomous passenger vehicles," in *Proc. 14th Int. IEEE Conf. Intell. Transp. Syst. (ITSC)*, Oct. 2011, pp. 1459–1464.

[10] D.-L. Chen and G.-P. Liu, "Coordinated path-following control for multiple autonomous vehicles with communication time delays," *IEEE Trans. Control Syst. Technol.*, vol. 28, no. 5, pp. 2005–2012, Sep. 2020.

[11] L. Nehaoua and L. Nouvelière, "Backstepping based approach for the combined longitudinal-lateral vehicle control," in *Proc. IEEE Intell. Vehicles Symp.*, Jun. 2012, pp. 395–400.

[12] A. Ferdowsi, S. Ali, W. Saad, and N. B. Mandayam, "Cyber-physical security and safety of autonomous connected vehicles: Optimal control meets multi-armed bandit learning," *IEEE Trans. Commun.*, vol. 67, no. 10, pp. 7228–7244, Oct. 2019.

[13] K. Koscher et al., "Experimental security analysis of a modern automobile," in *The Ethics of Information Technologies*. Evanston, IL, USA: Routledge, 2020, pp. 119–134.

[14] S. Xiao, X. Ge, Q.-L. Han, and Y. Zhang, "Secure distributed adaptive platooning control of automated vehicles over vehicular ad-hoc networks under denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 52, no. 11, pp. 12003–12015, Nov. 2022.

[15] S. Xiao, X. Ge, Q.-L. Han, and Y. Zhang, "Secure and collision-free multi-platoon control of automated vehicles under data falsification attacks," *Automatica*, vol. 145, Nov. 2022, Art. no. 110531.

[16] N. Zhao, X. Zhao, M. Chen, G. Zong, and H. Zhang, "Resilient distributed event-triggered platooning control of connected vehicles under denial-of-service attacks," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 6, pp. 6191–6202, Mar. 2023.

[17] X.-M. Zhang, Q.-L. Han, X. Ge, and L. Ding, "Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3616–3626, Aug. 2020.

[18] R. Merco, F. Ferrante, and P. Pisu, "A hybrid controller for DOS-resilient string-stable vehicle platoons," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 3, pp. 1697–1707, Mar. 2021.

[19] X. Ge, Q.-L. Han, Q. Wu, and X.-M. Zhang, "Resilient and safe platooning control of connected automated vehicles against intermittent denial-of-service attacks," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 5, pp. 1234–1251, May 2023.

[20] D. Ding, Q.-L. Han, X. Ge, and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey," *IEEE Trans. Syst. Man, Cybern., Syst.*, vol. 51, no. 1, pp. 176–190, Jan. 2021.

[21] Z. A. Biron, S. Dey, and P. Pisu, "Resilient control strategy under denial of service in connected vehicles," in *Proc. Amer. Control Conf. (ACC)*, May 2017, pp. 4971–4976.

[22] Z. A. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, Dec. 2018.

[23] E. Mousavinejad, F. Yang, Q.-L. Han, X. Ge, and L. Vlacic, "Distributed cyber attacks detection and recovery mechanism for vehicle platooning," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 9, pp. 3821–3834, Sep. 2020.

[24] D. Zhang, Y. Shen, S. Zhou, X. Dong, and L. Yu, "Distributed secure platoon control of connected vehicles subject to DoS attack: Theory and application," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 51, no. 11, pp. 7269–7278, Nov. 2021.

[25] Y. Wang, N. Bian, L. Zhang, Y. Huang, and H. Chen, "Resilient path-following control of autonomous vehicles subject to intermittent denial-of-service attacks," *IET Intell. Transp. Syst.*, vol. 15, no. 12, pp. 1508–1521, Dec. 2021.

[26] H. Sun, C. Peng, and F. Ding, "Self-discipline predictive control of autonomous vehicles against denial of service attacks," *Asian J. Control*, vol. 24, no. 6, pp. 3538–3551, Nov. 2022.

[27] H.-T. Sun, P. Zhang, and C. Peng, "Output-sensitive event-triggered path following control of autonomous ground vehicles under stochastic FDI attacks," *J. Franklin Inst.*, vol. 360, no. 3, pp. 2307–2325, Feb. 2023.

[28] H.-T. Sun and C. Peng, "Event-triggered adaptive security path following control for unmanned ground vehicles under sensor attacks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 7, pp. 1–10, Oct. 2023.

[29] R. Wang, H. Jing, C. Hu, F. Yan, and N. Chen, "Robust H_∞ path following control for autonomous ground vehicles with delay and data dropout," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 7, pp. 2042–2050, Jul. 2016.

[30] R. Skjetne and T. I. Fossen, "Nonlinear maneuvering and control of ships," in *Proc. MTS/IEEE Oceans. Ocean Odyssey. Conf.*, Nov. 2001, pp. 1808–1815.

[31] Q. Wang, W. Tai, Y. Tang, H. Zhu, M. Zhang, and D. Zhou, "Coordinated defense of distributed denial of service attacks against the multi-area load frequency control services," *Energies*, vol. 12, no. 13, p. 2493, Jun. 2019.

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

[33] H. Shisheh Foroush and S. Martínez, "On triggering control of single-input linear systems under pulse-width modulated dos signals," *SIAM J. Control Optim.*, vol. 54, no. 6, pp. 3084–3105, 2016.

[34] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Analysis of stochastic switched systems with application to networked control under jamming attacks," *IEEE Trans. Autom. Control*, vol. 64, no. 5, pp. 2013–2028, May 2019.

[35] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, Nov. 2015.

[36] Y. Ma, Z. Nie, S. Hu, Z. Li, R. Malekian, and M. Sotelo, "Fault detection filter and controller co-design for unmanned surface vehicles under DoS attacks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 3, pp. 1422–1434, Mar. 2021.

[37] S. Hu, D. Yue, X. Xie, X. Chen, and X. Yin, "Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks," *IEEE Trans. Cybern.*, vol. 49, no. 12, pp. 4271–4281, Dec. 2019.

[38] W. Yu, S. Hu, X. Chen, and Y. Ma, "Attack parameter dependent H8 path following control design for autonomous vehicles under periodic DoS attacks," in *Proc. 41st Chin. Control Conf. (CCC)*, Jul. 2022, pp. 5475–5480.

[39] Y. Tang, X. Luo, Q. Hui, and R. K. C. Chang, "Modeling the vulnerability of feedback-control based Internet services to low-rate DoS attacks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 3, pp. 339–353, Mar. 2014.

[40] G. Macia-Fernandez, J. E. Diaz-Verdejo, and P. Garcia-Teodoro, "Mathematical model for low-rate DoS attacks against application servers," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 519–529, Sep. 2009.

[41] W.-H. Chen, J. Zhong, and W. X. Zheng, "Delay-independent stabilization of a class of time-delay systems via periodically intermittent control," *Automatica*, vol. 71, pp. 89–97, Sep. 2016.

[42] S. Hu, X. Ge, X. Chen, and D. Yue, "Resilient load frequency control of islanded AC microgrids under concurrent false data injection and denial-of-service attacks," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 690–700, Jan. 2023.

Songlin Hu (Member, IEEE) received the Ph.D. degree in engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2012. Since 2013, he has been with the College of Automation, Nanjing University of Posts and Telecommunications, Nanjing, China. He is currently a Professor with the Institute of Advanced Technology for Carbon Neutrality, Nanjing University of Posts and Telecommunications. His research interests include model/data-based networked control, smart grids, multi-agent systems, and reinforcement learning.

Yong Ma (Member, IEEE) received the B.Sc. degree from Wuhan University of Technology (WUT), China, in 2006, the M.Sc. degree from Dalian Maritime University, China, in 2008, and the Ph.D. degree from the Huazhong University of Science and Technology, China, in 2012. He is currently a Full Professor with the Department of Maritime Management, School of Navigation, WUT. His current research interests include intelligent algorithms, systems, and platforms for surface vessel navigation and control.

Xin Qi received the B.E. degree in automation and the master's degree in transportation engineering from Wuhan University of Technology (WUT), Wuhan, China, in 2020 and 2023, respectively. His current research interests include networked control systems and event-triggered control for unmanned surface vehicles.

Zhixiong Li (Senior Member, IEEE) received the Ph.D. degree in transportation engineering from Wuhan University of Technology, China, in 2013. He is currently with the Faculty of Mechanical Engineering, Opole University of Technology, Poland. His research interests include intelligent vehicles and control, loop closure detection, and mechanical system modeling and control.

Reza Malekian (Senior Member, IEEE) is currently with the Department of Computer Science and Media Technology, Malmö University, Malmö, Sweden. His current research interests include the Internet of Things and sensors in intelligent transportation systems. He is a member of the IEEE Signal Processing Society Chapters Committee and the Co-Founder of the IEEE Vehicular Technology Society (VTS) South Africa Chapter.

Miguel Angel Sotelo (Fellow, IEEE) received the Ph.D. degree in electrical engineering from the University of Alcalá (UAH), Madrid, Spain, in 2001. He is currently a Full Professor with the Department of Computer Engineering, UAH. His research interests include autonomous vehicles and prediction of intentions.