文章编号：0253-374X(2022)12-1715-13

DOI：10.11908/j.issn.0253-374x.22406

一种网络攻击下网联自动车的改进换道模型

吴新开[1]，何　山[1]，张少伟[1]，贺晓征[2]，王斯奋[1]

(1. 北京航空航天大学交通科学与工程学院 北京 100191；2. Department of Civil and Environmental Engineering，Rensselaer Polytechnic Institute，Troy，NY 12180，United States)

摘要：网联自动车被认为可以提升交通效率、保证行车安全并节约能源，但是由于无线通信系统的开放性，网联自动车很容易受到网络攻击的威胁。现有的研究主要集中于网络攻击的种类及过程，并评估该攻击对车辆纵向行为的影响。本文旨在研究网络攻击对车辆横向行为的影响，即对网络攻击下的换道行为进行研究。通过对经典的跟驰模型智能驾驶员模型(Intelligent Driver Model，IDM)和经典的换道模型最小化换道总制动模型(Minimizing Overall Braking Induced by Lane changes，MOBIL)进行改进，提出了一种扩展换道模型(Extended Lane—Changing model，ELC)，来对网络攻击影响下的车辆换道行为进行建模分析。最后通过仿真实验，说明了不同的恶意网络攻击对车辆换道行为的影响。结果表明，网络攻击会显著影响车辆的换道决策，并导致异常驾驶行为。

关键词：网联自动车；换道行为；网络攻击；最小化换道总制动模型；智能驾驶员模型

中图分类号：U461.6　　**文献标志码**：A

An Improved Lane-changing Model for Connected Automated Vehicles Under Cyberattacks

WU Xinkai[1]，*HE Shan*[2]，*ZHANG Shaowei*[1]，*HE Xiaozheng*[1]，*WANG Sifen*[1]

(1. School of Transportation Science and Engineer Beihang University，Beijing 100191，China；2. Department of Civil and Environmental Engineering，Rensselaer Polytechnic Institute，Troy，NY 12180，United States)

Abstract：The connected automated vehicle (CAV) is promising to enhance traffic efficiency，traveling safety，and energy savings. However，due to the open wireless communication，the CAV is vulnerable to cyber threats. Existing studies mainly focus on surveying related cyberattacks and evaluating the impact of attacks on vehicular longitudinal behaviors on a single lane. This paper aims to investigate the effects of cyberattacks on vehicular lateral behaviors on a two-lane highway，*i.e.*，the lane-changing (LC) behaviors under cyberattacks. Based on a classical lane-changing model--minimizing overall braking induced by lane changes (MOBIL) model，and a classical car-following model--Intelligent Driver Model (IDM)，this study proposes an extended lane-changing model (ELC) which can model CAV′s lane-changing behaviors under cyberattacks. At the end，simulations are conducted to illustrate the impact of different malicious attacks on vehicles′ LC movements. Results show that cyberattacks can imperil the LC maneuvers and lead to abnormal driving behaviors.

Key words：connected automated vehicles；lane-changing；cyberattacks；MOBIL model；intelligent driver model

Connected automated vehicles (CAVs)，which integrate vehicle-to-vehicle (V2V) communication and autonomous vehicles (AV) technologies，are expected to greatly improve traffic safety and efficiency [1-2]. Through wireless communication，CAVs can share and exchange information such as velocity，position，acceleration，and road conditions [3]. However，due to open wireless communication，CAVs are vulnerable to various kinds of attacks，such as *man—in—the—middle attack*，*impersonation attack*，*forging attack*，*replay attack*，and *Sybil attack* [4-5]. These cyberattacks have shown severe risks to CAV traffic. To prevent these risks，a fundamental task is to research the impacts of cyberattacks on CAVs′ driving behaviors [6-7].

Lopez *et al.* [8] developed attack models as

收稿日期：2022-10-20
基金项目：国家自然科学基金青年基金(52002013)；国家自然科学基金面上项目(61773040)
第一作者：吴新开(1979—)，博士，教授. 研究方向为智能交通系统、自动驾驶、电动汽车及汽车信息安全。
E-mail：xinkaiwu@buaa.edu.cn

functions of tampered traffic control settings (*e. g.*, green time raios, cycle length, retaining ratios) with outputs equivalent to mobility impacts on the traffic network. Feng *et al.* [9] investigated the vulnerability of traffic control systems in a connected environment and summarized four attack surfaces, including signal controllers, vehicle detectors, roadside units, and onboard units. Khan *et al.* [10] developed a conceptual system dynamics (SD) model to analyze cybersecurity in the complex, uncertain deployment of CAVs. The SD model consists of six critical avenues and maps their respective parameters that either trigger or mitigate cyber-attacks in the operation of CAVs using a systematic theoretical approach. Maglaras *et al.* [11] present main threats to critical infrastructures along with protective measures that one nation can take, and which are classified according to legal, technical, organizational, capacity building, and cooperation aspects. Dong *et al.* [12] designed an evaluation framework for cyberattacks on CAVs, and analyzed the impact of cyberattacks on vehicles and the transportation system. Li *et al.* [13] investigated the influence of slight cyber-attacks on the longitudinal safety of CAVs, and considered the communicated position and speed data from preceding CAVs under attacks. Hu *et al.* [14] proposed a method to detect cyberattacks by cross-checking Signal Phase and Timing (SPaT) information and connected vehicle trajectories data.

However, the existing work aims to investigate the impact of cyberattacks on CF behaviors. To the best of our knowledge, only a few previous studies have considered the impact of cyberattacks on LC behaviors. For instance, Khattak *et al.* [15] utilized an infrastructure-based communication platform consisting of cooperative adaptive cruise control and lane control to perform cyber risk assessments of CAVs. Kashyap *et al.* [16] found that the malicious vehicles may perform subtle speed and/or lane changes and modeled the mix of malicious and normal vehicles in the traffic system by using the Lighthill-Whitham-Richards (LWR) model. The authors aimed to use Gaussian Processes to detect the presence of such malicious vehicles in such a mixed traffic scenario. Zhao *et al.* [17] used the default lane-changing algorithm in Simulation of Urban Mobility (SUMO) and presented the traffic behavior under cyberattacks.

Although these studies present the influence of cyberattacks on LC behaviors using simulation experiments, they have not developed new lane-changing model with cyberattacks. In this research, we aim to construct an improved LC model associated with cyberattacks, through which we could better understand how the cyberattacks impact the LC maneuver and how to quantify this impact. The detailed description will be presented in the following sections.

This study improves a classic LC model, *i. e.*, MOBIL (Minimizing Overall Braking Induced by Lane changes) model [18] to describe the lane-changing behavior. In the proposed ELC (Extended Lane Change) model, an improved IDM (Intelligent Driver Model), a most widely used CF model [19], is adopted to derive neighbor vehicles′ accelerations based on their own and their nearest leaders' velocities and positions when the LC happens. Numerical simulations are conducted to verify the effectiveness of our proposed ELC models and illustrate the impact of cyberattacks including velocity, position and acceleration attacks on LC behaviors.

The main contributions are described as below. (i) Cyberattacks on vehicles are formulized and integrated into the classical LC and CF models. (ii) The extended LC model and the improved IDM are used to describe the process of LC in two lanes. (iii) Various cyberattacks are classified into three types, *i. e.*, velocity, position and acceleration attacks, and numerical simulations illustrate the changes of malicious attacks on vehicles′ LC movements.

1 An extended lane-changing model for CAVs under cyberattacks

1.1 Lane-changing model

In general, a LC process consists of three phases, *i. e.*, before, during, and after the lane change [20]. In the phases of before and after the lane

change, vehicles follow the CF rules. Also, before the lane change, the subject vehicle requires to consider neighbor vehicles′ dynamical parameters such as velocity, space gap, and acceleration. If the LC condition is satisfied, then the subject vehicle performs a lane change. This section presents how to derive an extended lane-changing (ELC) model with cyberattacks.

To describe CAVs′ LC behaviors under cyberattacks, we adopt the MOBIL model, which has many advantages [21-22] compared to other LC models. The most evident one is that MOBIL uses acceleration as a model control variable, which allows perfect integration with other CF models to simulate both CF and LC behaviors at a microscopic level. Also, MOBIL integrates the LC demand generation and the feasibility judgment, which can better describe CAVs′ LC behaviors.

In this study, the MOBIL LC model is implemented to model a two-lane highway traffic. A simple diagram of a lane change on two-lane traffic is first provided in Fig. 1. As shown in the figure, the subject vehicle, indexed as m, plans to change to its neighbor lane. Before the LC, its nearest preceding and following vehicles are indexed as $m-1$ and $m+1$, respectively. The neighbor vehicles on the LC target lane are indicated by n and $n-1$, respectively. When the LC condition is satisfied, the subject vehicle m will change its current lane to the neighbor target lane, as shown by the virtual vehicle in Fig. 1. After the lane change, the subject vehicle m follows its new preceding vehicle $n-1$ based on the CF theory. Meanwhile, the new follower of the subject vehicle turns to be vehicle n.

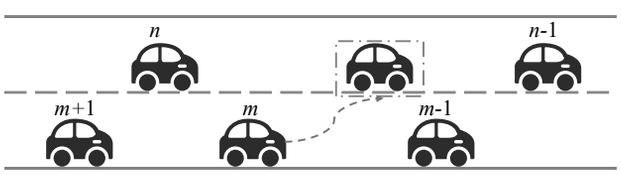

Fig. 1　A typical lane-changing scene

The MOBIL model has a comprehensive consideration of both LC safety and gain. Therefore, it needs to meet the following two essential conditions:

(1) The safety criterion: This condition aims to ensure the safety after the LC, *i. e.* both the accelerations of the subject vehicle m and its new follower vehicle n need to fit the following conditions:

$$a_m^{\mathrm{pre}} \geqslant -b_{\mathrm{safe}} \quad \text{and} \quad a_n^{\mathrm{pre}} \geqslant -b_{\mathrm{safe}} \tag{1}$$

where $a_m^{\mathrm{pre}}$and a_n^{pre} represent the predicted accelerations of the subject vehicle m and its new follower vehicle n after the subject vehicle m changes the lane, respectively; and b_{safe} represents a maximum safe deceleration.

(2) The incentive condition: This criterion is used to decide whether a lane change improves the local traffic status. The incentive criterion is formalized as below:

$$\underbrace{a_m^{\mathrm{pre}} - a_m}_{\text{subject vehicle}} + p\left(\underbrace{a_n^{\mathrm{pre}} - a_n}_{\text{new follower}} + \underbrace{a_{m+1}^{\mathrm{pre}} - a_{m+1}}_{\text{old follower}}\right) > \Delta a_{\mathrm{th}} \tag{2}$$

where a_m indicates the acceleration of vehicle m on the current lane, p denotes the politeness factor, a_{m+1}^{pre} indicates the predicated acceleration of vehicle $m+1$ after the subject vehicle m changes the lane, and Δa_{th} is the LC threshold. The politeness factor p can be interpreted as the degree of altruism, which is a variable that determines the impact of nearby vehicles on the LC decision of the subject vehicle. It can vary from $p=0$ for completely selfish lane-changers to $p>1$ for altruistic drivers who do not change lane if LC would deteriorate the traffic situation considering these followers. Furthermore, $p>0$ represents considering the benefits of other vehicles.

1.2　Car-following model

There are two different car-following models, linear and the other nonlinear model, to demonstrate the CAVs′ following behaviors. Car-following models are used to formulate vehicle interactions and uncover CAV platoon dynamics. Linear car-following models include Pipes model, Helly′s model, and Gazis - Herman - Rothery model. Nonlinear car-following models include Newell′s model, optimal velocity model, and intelligent driver model (IDM). The critical difference between these two types of car-following models is that the nonlinear models capture a nonlinear relationship with deviation from the desired space gap and the relative velocity.

Compared to the linear car-following model, the

nonlinear car-following is more suitable for describing the real traffic flow due to its nonlinearity and sophistication in capturing complex vehicle dynamics. This research adopts the IDM due to its advantages as follows. First, the IDM is a multi-regime model, which presents a greater realism than other nonlinear models when characterizing the congested traffic flow [2]. Second, the IDM ensures collision-free vehicle movements, which would not cause unrealistic acceleration/deceleration shown in some linear car following models [23]. The formulation of this model is expressed as follows [19]:

$$a_m(t)=a\left(1-\left(\frac{v_m}{v_0}\right)^4-\left(\frac{s^*(v_m,\Delta v_m)}{s_m}\right)^2\right) \quad (3)$$

$$\text{with } s^*(v_m,\Delta v_m)=s_0+v_mT+\frac{v_m\Delta v_m}{2\sqrt{ab}}$$

where a_m indicates the acceleration of vehicle m; v_0 indicates the desired velocity in free flow; s^* indicates the desired safe gap; s_0 denotes the space gap in completely stopped traffic; $s_m=x_{m-1}-x_m-l$ is the space gap between the preceding vehicle $m-1$ and vehicle n; l is the length of vehicle; x_m is the position of the vehicle m; v_m is the velocity of vehicle m; and $\Delta v_m=v_m-v_{m-1}$ is the relative velocity between vehicle m and its preceding vehicle $m-1$. In addition, T is the desired time gap between successive vehicles; and a and b indicate the vehicle′s maximum acceleration and deceleration, respectively. Note if all vehicles travel uniformly, *i. e.*, each vehicle′s acceleration is equal to zero, each vehicle keeps the same velocity and space gap between consecutive vehicles.

In a normal CAV environment, each vehicle can receive dynamic information such as velocity, position, and acceleration from the surrounding vehicles. Vehicles′ information will be accurately sent to the target vehicle on time. However, when an attack happens, the information transmission between vehicles could be interrupted, delayed, lost, or even falsified. Then, the vehicle′s LC and CF behaviors can also be influenced. Note that this study only the V2V communication.

1.3 Cyberattacks

Much research has demonstrated that cyberattacks have an impact on the effective use of vehicles [24]. If without any influence of cyberattacks, vehicle dynamics information, including speed, acceleration, headway, etc., will be accurate and timely disseminated to other vehicles. The cyberattacks can be classified into three main categories: DoS attacks, replay attacks and false data injection attacks. When an attack such as spoofing, replay, and impersonation occurs, the information transmission among vehicles could be interrupted and/or falsified. A detailed description of these attacks is listed below [25-26].

(1) Spoofing attack: An adversary can compromise a vehicle and send fake messages such as fake location, velocity, and acceleration. For instance, GPS is responsible for delivering the real-time location message to the surrounding vehicles. When the spoofing attack happens, the spoofed GPS can send a fake location to the subject vehicle by releasing a strong-power signal from the GPS satellite simulator.

(2) Replay attack: An attacker captures the packets and replays them at a later time to disguise that they were sent by the true sender. Thus, the repeated message, which is sent after a while, could be accepted as a new message. Mathematically, the position, velocity, and position of vehicle may be unchanged during the attacking period.

(3) Impersonation attacks: In vehicular networks, an attacker could impersonate a roadside infrastructure or vehicle to trick others by applying their authentication details. For example, an attacker might impersonate an emergency vehicle, which would give them a higher priority within the vehicular network and result in less congestion. The position, velocity, and position of vehicle can be altered.

The above cyberattacks could affect vehicles′ behaviors in their own manners. Essentially, all these attacks can release bogus messages which falsify the vehicle′s dynamic information such as velocity, position, and acceleration. Hence, for simplicity, this research considers all these attacks as *bogus*

attacks [25].

1.4 Extended LC model with cyberattacks

To describe CAVs′ dynamic traffic behaviors under cyberattack, we present the following two representative attacking cases. In the first case, we assume that the velocity and/or the position of the preceding vehicle $m-1$ of the subject vehicle m is attacked, and vehicle $m-1$ sends falsified velocity and/or position messages to the subject vehicle m. Then the subject vehicle′s acceleration will be influenced. In this case, the influenced acceleration in MOBIL needs to be updated by the following extended IDM model:

$$a_m(t)=a\left(1-\left(\frac{v_m}{v_0}\right)^4-\left(\frac{s^*(v_m,v_m-\beta v_{m-1})}{\gamma x_{m-1}-x_m-l_m}\right)^2\right) \tag{4}$$

where β and γ are the weight parameters to describe the impacts of cyberattacks on velocity and position of the subject vehicle's nearest leader, respectively. If $\beta\neq 0$ or $\gamma\neq 0$, Eq. (4) means that the velocity or the position of vehicle $m-1$ is attacked. If $\beta=\gamma=0$, Eq. (4) is transformed to the classical IDM model.

In the second case, we assume that the acceleration of the following vehicle n after LC of the subject vehicle m is falsified. In this situation, the weighting parameters α, δ are introduced to capture the change of acceleration influenced by attacks. An improved incentive criterion in the MOBIL model under cyberattacks can be formulated below:

$$\underbrace{a_m^{\text{pre}}-a_m}_{\text{subject vehicle}}+p\left(\underbrace{a_n^{\text{pre}}-\alpha a_n}_{\text{new follower}}+\underbrace{a_{m+1}^{\text{pre}}-\delta a_{m+1}}_{\text{old follower}}\right)>\Delta a_{\text{th}} \tag{5}$$

where α and δ are the weighting parameters to describe the impacts of cyberattacks on the new follower vehicle n after LC and the old follower vehicle $m+1$ before LC. Here, α and δ have clear physical meanings. If $\alpha=\delta=1$, it indicates the CAV is moving without cyberattacks. While $\alpha\neq 1$ and/or $\delta\neq 1$, it denotes the CAV is influenced by cyberattacks. Specifically, if $\alpha>1$ ($\delta>1$), it represents that the subject vehicle receives overestimated acceleration messages of the following vehicle after (or before) LC; and if $\alpha<1$ ($\delta<1$), it represents that the subject vehicle receives an underestimated acceleration message from the following vehicle after (or before) LC.

Overall, these falsified messages could cause the vehicle to make the wrong decision, leading to potential collisions. To fully capture these impacts, based on above Eqs. (1), (4) and (5), we can derive an ELC model, *i. e.*, an improved MOBIL model, as described in the following equation:

$$\begin{cases} a_m^{\text{pre}}\geqslant -b_{\text{safe}} \\ a_n^{\text{pre}}\geqslant -b_{\text{safe}} \\ \underbrace{a_m^{\text{pre}}-a_m}_{\text{subject vehicle}}+p\left(\underbrace{a_n^{\text{pre}}-\alpha a_n}_{\text{new follower}}+\underbrace{a_{m+1}^{\text{pre}}-\delta a_{m+1}}_{\text{old follower}}\right)>\Delta a_{\text{th}} \\ a_n(t)=a\left(1-\left(\dfrac{v_n}{v_0}\right)^4-\left(\dfrac{s^*(v_n,v_n-\beta v_{n-1})}{\gamma x_{n-1}-x_n-l_n}\right)^2\right) \end{cases} \tag{6}$$

Note that Eq. (6) essentially integrates the CF IDM model and the LC MOBIL model for the CAVs under attacks. The following section will verify the effectiveness of our proposed model.

2 Numerical Simulation

This section presents a series of simulations to verify the effectiveness of the proposed ELC model and illustrate the impact of cyberattacks on vehicles′ LC behaviors. In this study, we use Python to show the change in vehicles′ behaviors under cyberattacks. We select a two-lane highway whose length is long enough to conduct our simulation. The total simulation time is 30 s, and each sampling time is 0.01 s. For the convenience of investigation, we put forward the following assumptions (see Fig. 2): (i) 12 CAVs are grouped as two platoons and are traveling on a straight two-lane highway; (ii) Without LC, each vehicle updates its dynamical parameters based on the IDM model and adopts a simple predecessor-following communication protocol, *i. e.*, one vehicle only receives beacon messages from its directly preceding vehicle; and (iii) The subject vehicle (3rd vehicle) changes to the neighbor lane based on the proposed ELC Eq. (6).

To illustrate the impact of cyberattacks on the vehicle′s lateral behaviors, we design five scenarios: without attacks, velocity attack, position attack,

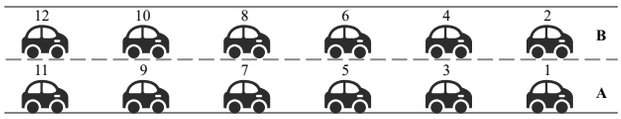

Fig. 2 Numerical simulation scenarios

velocity and position attacks, and acceleration attack.

In all scenarios, each vehicle's initial space headway in the platoon is 35 m, and the initial velocity is set as 14 $m \cdot s^{-1}$. As shown in Fig. 2, the velocity of the first vehicle (*i. e.*, vehicle 1) in the current lane (*i. e.*, lane A) remains unchanged at 14 $m \cdot s^{-1}$, and the first vehicle (*i. e.*, vehicle 2) in the target lane (*i. e.*, lane B) is 18 $m \cdot s^{-1}$. Other vehicles in the platoon obey the IDM to follow their preceding vehicles. The initial values of all parameters for simulation are presented in Tab. 1.

Tab. 1 Simulation parameters

Parameter	Value	Description
N	12	Number of vehicles
$v_0/(m \cdot s^{-1})$	33.33	Desired free-flow velocity
T/s	1.6	Safety time headway
s_0/m	2	Jam distance
$a_i/(m \cdot s^{-2})$	0.73	Maximum acceleration
$b_i/(m \cdot s^{-2})$	1.67	Desired deceleration
$b_{safe}/(m \cdot s^{-2})$	4	Maximum safety deceleration
$\Delta a_{th}/(m \cdot s^{-2})$	0.1	Switching threshold
p	0.1	Politeness factor

(1) **Without cyberattacks**

As a reference, Fig. 3 shows the changes in the dynamic parameters of the platoon without cyberattacks. When the LC model does not meet the safety constraint and the incentive condition, there is no LC.

Before the LC, each vehicle is traveling uniformly in the current lane. We can see that the 3rd vehicle changes its lane at 6.23 s according to the classical MOBIL model. At this time, the 3rd vehicle's velocity is 14.44 $m \cdot s^{-1}$, and the 4th vehicle's velocity is 17.63 $m \cdot s^{-1}$. As shown in this figure, after the LC, the following vehicles of the 3rd vehicle in lane A (*e. g.*, 5th and 7th vehicles) accelerates to shrink the space headway. Meanwhile, the following vehicles of the 3rd vehicle in lane B (*e. g.*, 4th and 6th vehicles) have to decelerate to keep the safe space headway.

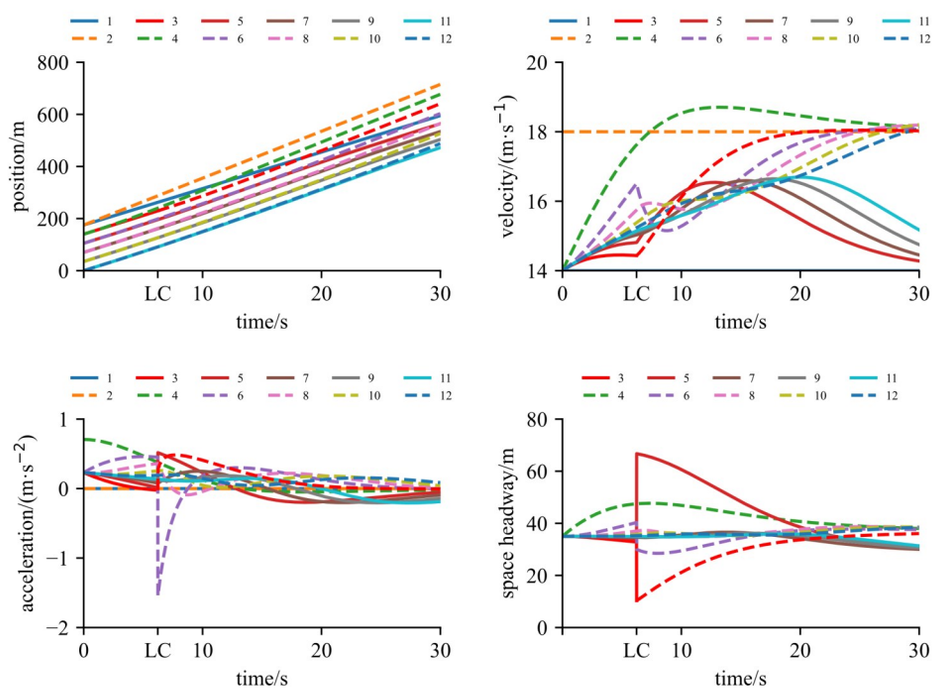

Fig. 3 Plots of position, velocity, acceleration, and space headway without attacks

(2) **Velocity attacks**

Fig. 4 and Fig. 5 show the dynamic parameters of the platoon when the 1st vehicle's velocity is underestimated ($\beta = 0.9$) and overestimated ($\beta = 1.1$), respectively. It can be seen that the 3rd vehicle plans to change its lane at 4.87 s and 7.80 s,

respectively. According to the extended IDM model Eq. (4), when the 1st vehicle's velocity is underestimated, the 3rd vehicle is forced to slow down to achieve safe space headway. Based on Eq. (2), the incentive value in the MOBIL model turns large. Hence, the subject vehicle (*i. e.*, 3rd vehicle) will change to the neighbor lane in advance. Compared with Fig. 3, under underestimated velocity attack, the LC time is advanced by 1.36 s.

Fig. 5 shows the impact of an overdamped velocity attack on the LC of the subject vehicle. If the released messages of the 1st vehicle's velocity are falsified and amplified, the subject vehicle (*i. e.*, 3rd vehicle) who receives the falsified messages has to accelerate to keep the same velocity as the first vehicle. Based on Eq. (2), the incentive value in the MOBIL model turns small. In this case, the LC time is delayed by 1.57 s. It should be noted that the real velocity of the first vehicle does not change. It is not difficult to imagine that this attack could lead to a potential collision.

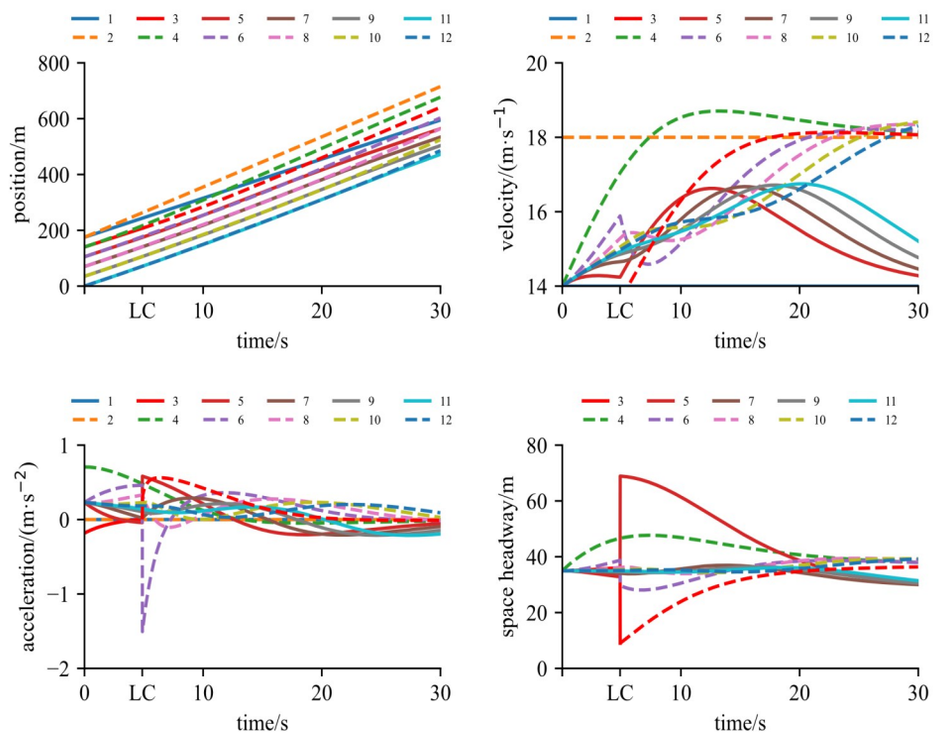

Fig. 4　Plots of position, velocity, acceleration, and space headway under underestimated velocity attacks when $\beta=0.9$

(3) Position attacks

Fig. 6 and Fig. 7 show changes in the dynamic parameters of the platoon when the space headway between the 1st vehicle and the 3rd vehicle is underestimated and overestimated, respectively. It can be seen that the 3rd vehicle chooses to change lanes at 5.76 s and 6.67 s, respectively. Intuitively, when the space headway is underestimated, the 3rd vehicle has to decrease its velocity to keep a safe space headway. The smaller acceleration of the subject vehicle leads to a larger incentive value based on Eq. (2). Hence, based on the MOBIL model, the subject vehicle should change its lane in advance. As shown in Fig. 6, the LC time is advanced by 0.47 s. By contrast, when the space headway is overestimated, the 3rd vehicle accelerates to shorten the space headway. Based on Eq. (2), the larger acceleration of the subject vehicle leads to a smaller incentive value. Hence, based on the MOBIL model, the LC time of the subject vehicle should be postponed. As shown in Fig. 7, the lane-changing time is delayed by 0.44 s.

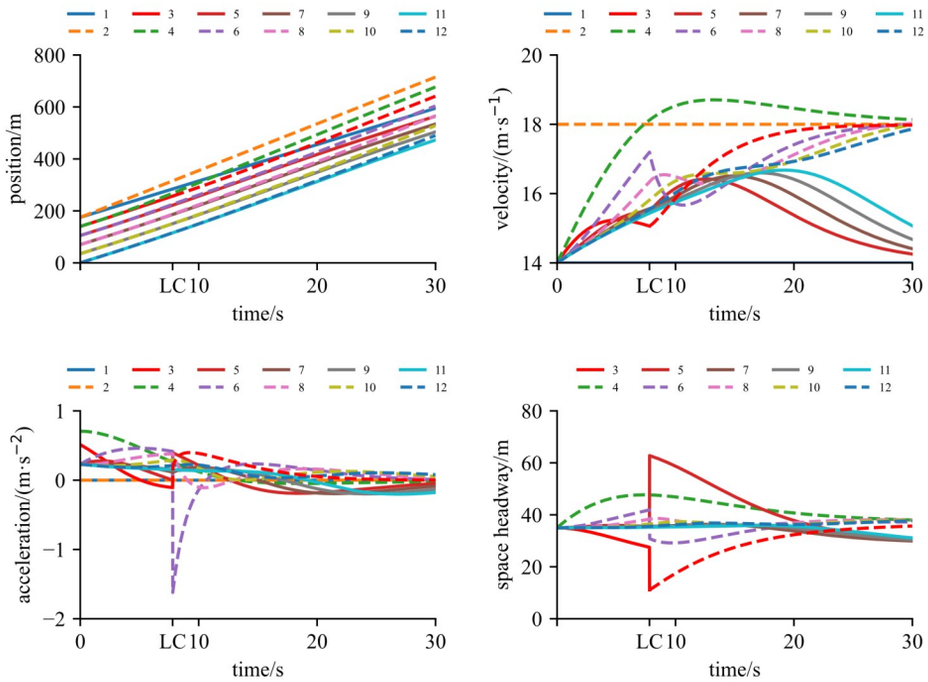

Fig. 5 Plots of position, velocity, acceleration, and space headway under overestimated velocity attacks when $\beta=1.1$

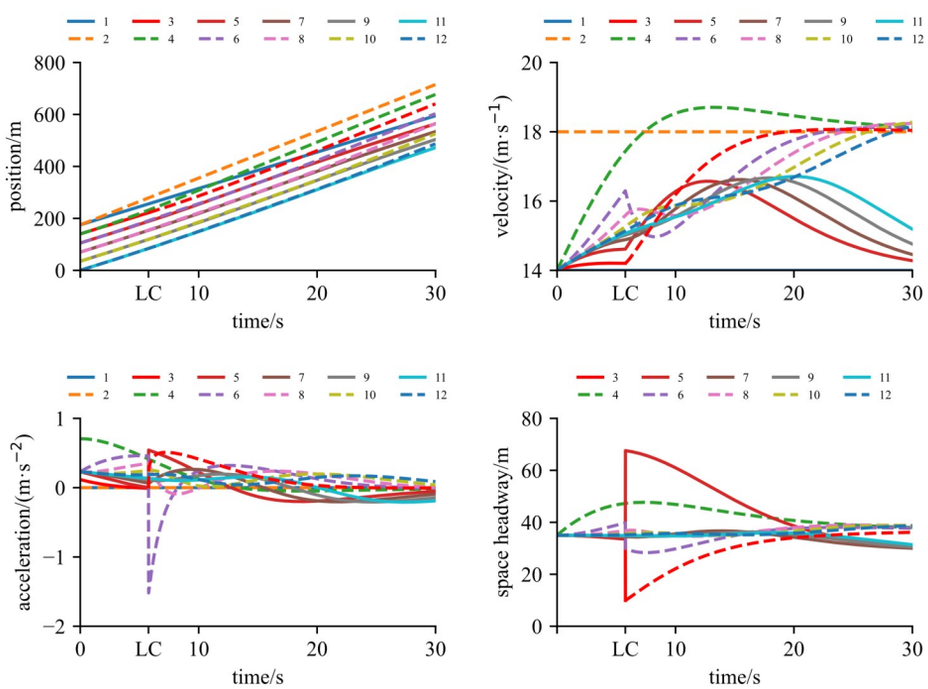

Fig. 6 Plots of position, velocity, acceleration, and space headway under underestimated position attacks when $\gamma=0.9$

(4) **Velocity and position attacks**

In this case, we discuss the effects of modification of both velocity and position on LC behaviors. Fig. 8 and Fig. 9 show that changes in position, velocity, acceleration, and space headway of the vehicle platoon under velocity and position

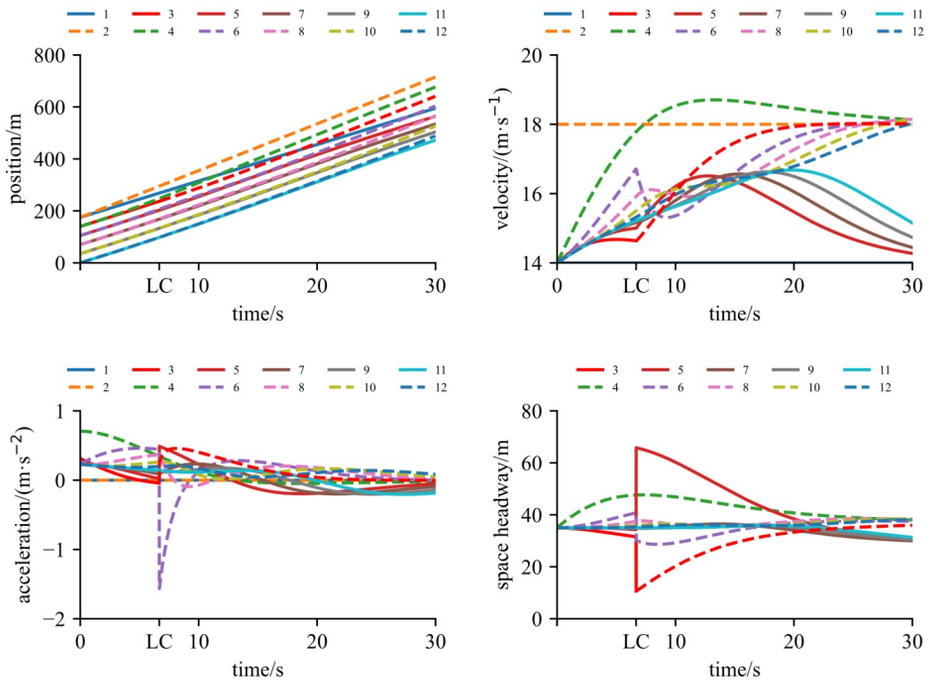

Fig. 7　Plots of position, velocity, acceleration, and space headway under overestimated position attacks when $\gamma=1.1$

attacks. The 3rd vehicle changes lanes at 4.42 s and 8.20 s, respectively. It can be seen that when the velocity and headway are both underestimated by 10%, *i. e.*, $\beta=\gamma=0.9$, the LC time will be greatly advanced by 1.81 s. Underestimated velocity and space headway lead to an increase in the incentive value of lane-changing. Thus the 3rd vehicle changes its lane quickly. When the velocity and headway are both overestimated by 10%, *i. e.*, $\beta=\gamma=1.1$, the 3rd vehicle first increases its velocity to follow the 1st vehicle and reduce the space headway, resulting in a decrease in the incentive value of LC based on Eq. (2). Hence, the LC time is put off. In this case, the LC time is delayed by 1.97 s. Compared with the velocity or position attacks, the influence of both velocity and position is much severer.

(5) Acceleration attack

To be consistent with the proposed ELC model, we assume that the accelerations of the new follower after LC (the 6th vehicle) and the old follower before LC (the 5th vehicle) are falsified. In detail, Fig. 10 and Fig. 11 show the changes in the dynamics parameters of the platoon when the acceleration is underestimated (*i. e.*, $\alpha=\delta=0.5$) and overestimated (*i. e.*, $\alpha=\delta=1.5$), respectively. These figures show that the 3rd vehicle changes its lane at 6.21 s and 6.25 s, respectively. In fact, the new or old followers cannot influence the subject vehicle's longitudinal behaviors but the lateral LC behaviors based on the MOBIL model. Compared with no attack scenarios scenario, whether underestimated or overestimated acceleration attacks could result in a slight change in LC time. The reason is that the politeness factor ($p=0.1$) in Eq. (6) weakens the influence of the accelerations of the new and old followers. Hence, acceleration attacks only lead to slight time changes.

The above five simulation experiments show that falsification of acceleration, velocity, and position will cause abnormal LC behavior, such as LC time in advance or delay and vehicles' oscillation amplitudes. These results demonstrated that cyberattacks could influence traffic efficiency and cause potential rear-end collisions.

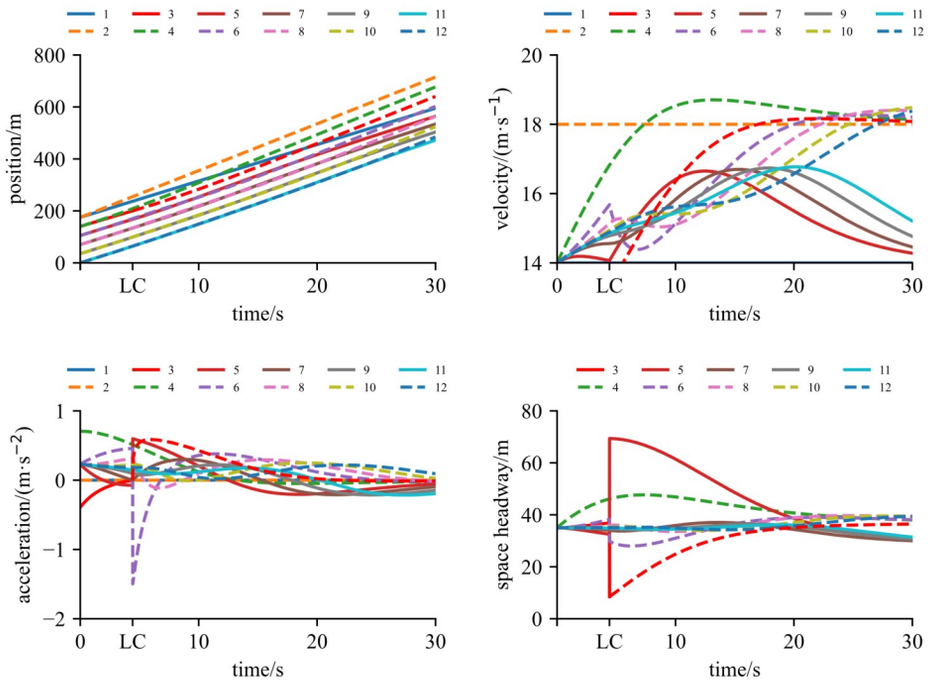

Fig. 8 Plots of position, velocity, acceleration, and space headway under underestimated velocity and position when $\beta=\gamma=0.9$

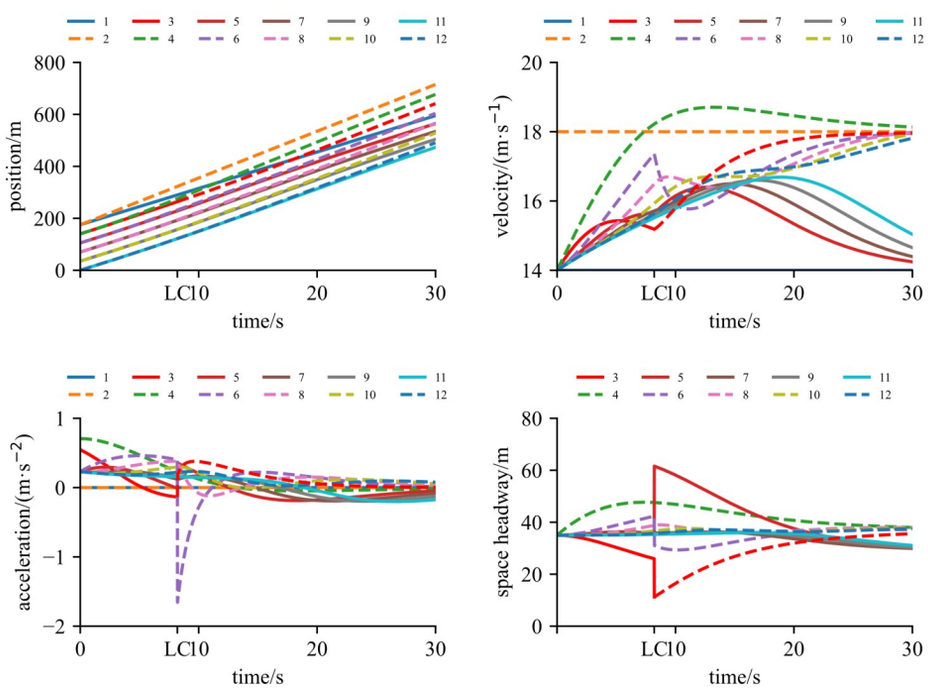

Fig. 9 Plots of position, velocity, acceleration, and space headway under overestimated velocity and position when $\beta=\gamma=1.1$

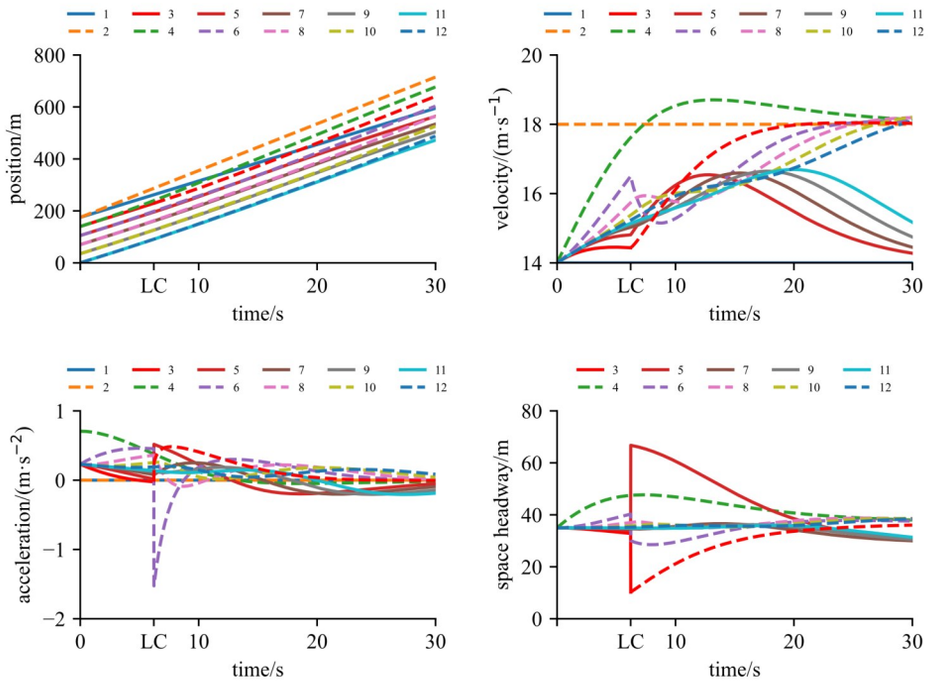

Fig. 10　Plots of position, velocity, acceleration, and space headway under underestimated acceleration attacks when $\alpha=\delta=0.5$

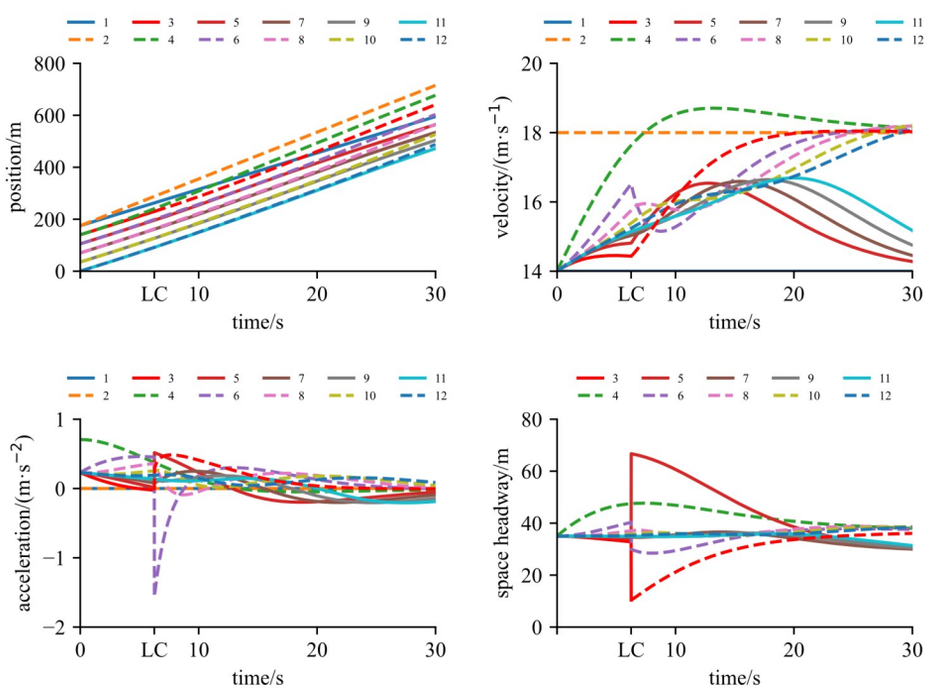

Fig. 11　Plots of position, velocity, acceleration, and space headway under overestimated acceleration attacks when $\alpha=\delta=1.5$

3 Conclusions

With the advent of intelligent and connected technology, the impacts of cyberattacks on vehicles have drawn many scholars′ attention. This research focuses on modeling LC behaviors under cyberattacks. To this end, based on the MOBIL and IDM models, this study proposes an extended LC (ELC) model with cyberattacks to describe the LC decision-making behavior. Through the numerical simulation, we found that cyberattacks could imperil the LC maneuvers and different attacks are able to result in different consequences such as LC time in advance or delay, and even potential rear-end collisions.

By studying the lane-changing behavior of connected vehicles under cyberattacks, the impact of cyberattacks on vehicle lane-changing behaviors is revealed. Attackers can attack with different parameters on vehicles according to different attack purposes and real-time traffic conditions to accomplish specific attack goals, such as causing collisions and increasing traffic congestion.

The research in this paper allows us to have a deeper understanding of the impact mechanism of cyberattacks, so that we can actively defend against attacks. By analyzing the manifestations and results of cyberattacks, the detection and defense of cyberattacks can be completed in time, so as to avoid personal and property hazards.

In actual vehicle applications, relevant algorithms can be installed to detect the dynamic information of the own vehicle and other vehicles, so as to quickly and timely find abnormal dynamic updates and communication information. At the same time, the detection method can also be used in combination with other cyberattacks detection methods to improve the detection rate of cyberattacks, and provide response strategies in time.

Vehicles have multiple strategies to defend against cyberattacks. In addition to cryptographic methods, communication information can also be verified by methods such as multi-sensor data fusion. At this time, the attacker needs more sophisticated attack strategies, such as performing compound attacks and attacking acceleration, speed, and position information at the same time, which also puts forward higher requirements for vehicle information security protection.

There are several directions for future study. First, it is expected that this research could help counter the detrimental effects caused by cyberattacks. By understanding the impacts on traffic dynamics caused by different cyberattacks, some possible traffic control, and management strategies could be developed and applied to resolve these impacts. Second, in this study, for the convenience of analysis, we just adopt two lane framework in our simulation studies, the framework will be extended to a multi-lane with thousands of vehicles. Third, it will be interesting to explore to assess the impact on more parameters like traffic flow, safety etc. At last, security work against malicious attacks such as detection of cyberattacks, privacy-preserving scheme between V2X and human driver intervention, etc. will be investigated in nearly future.

作者贡献声明:

吴新开:构建框架,起草论文;
何山:调研文献,提出模型;
张少伟:调试参数,设计实验;
贺晓征:实验仿真,验证模型;
王斯奋:评阅论文,提供指导。

参考文献:

[1] TIAN D, WU G, BORIBOONSOMSIN K, *et al*. Performance measurement evaluation framework and co-benefit/tradeoff analysis for connected and automated vehicles (cav) applications: a survey [J]. IEEE Intelligent Transportation Systems Magazine, 2018,10(3): 110.

[2] SARKER A, SHEN H, RAHMAN M, *et al*. A review of sensing and communication, human factors, and controller aspects for information-aware connected and automated vehicles [J]. IEEE Transactions on Intelligent Transportation Systems, 2019,21(1): 7.

[3] PAPADOULIS A, QUDDUS M, IMPRIALOU M. Evaluating the safety impact of connected and autonomous vehicles on motorways [J]. Accident Analysis & Prevention, 2019,124: 12.

[4] FERRAG M A, MAGLARAS L A, JANICKE H, *et al*.

Authentication protocols for internet of things: a comprehensive survey [J]. Security and Communication Networks, 2017, 2017: 1.

[5] ALNASSER A, SUN H, JIANG J. Cyber security challenges and solutions for v2x communications: a survey [J]. Computer Networks, 2019,151: 52.

[6] KHATTAK Z H, SMITH B L, FONTAINE M D. Impact of cyberattacks on safety and stability of connected and automated vehicle platoons under lane changes [J]. Accident Analysis & Prevention, 2021,150: 105861.

[7] HADDAD J, MIRKIN B. Resilient perimeter control of macroscopic fundamental diagram networks under cyberattacks [J]. Transportation research part B: methodological, 2020, 132: 44.

[8] LOPEZ A, JIN W, AL FARUQUE M A . Security analysis for fixed-time traffic control systems [J]. Transportation Research Part B: Methodological, 2020,139: 473.

[9] FENG Y, HUANG S, CHEN Q A, *et al*. Vulnerability of traffic control system under cyberattacks with falsified data [J]. Transportation research record, 2018, 2672(1): 1.

[10] KHALID KHAN S, SHIWAKOTI N, STASINOPOULOS P. A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles [J]. Accident Analysis & Prevention, 2022,165: 106515.

[11] MAGLARAS L, FERRAG M, DERHAB A, *et al*. Threats, countermeasures and attribution of cyber attacks on critical infrastructures [J]. EAI Endorsed Transactions on Security and Safety, 2018,5(16): 1.

[12] DONG C, WANG H, NI D, *et al*. Impact evaluation of cyber-attacks on traffic flow of connected and automated vehicles [J]. IEEE Access, 2020(8): 86824.

[13] LI Y, TU Y, FAN Q, *et al*. Influence of cyber-attacks on longitudinal safety of connected and automated vehicles [J]. Accident Analysis & Prevention, 2018,121: 148.

[14] HU J, QI L, ZHANG Z, *et al*. A detection method for cyber-attack on connected signal phase and timing information [J]. Transportmetrica B: Transport Dynamics, 2022,10(1): 731.

[15] KHATTAK Z H, SMITH B L, FONTAINE M D. Impact of cyberattacks on safety and stability of connected and automated vehicle platoons under lane changes [J]. Accident Analysis & Prevention, 2021,150: 105861.

[16] KASHYAP A, CHAKRAVARTHY A, MENON P P. Detection of cyber-attacks in automotive traffic using macroscopic models and gaussian processes [J]. IEEE Control Systems Letters, 2022,6: 1688.

[17] ZHAO X, ABDO A, LIAO X, *et al*. Evaluating Cybersecurity Risks of Cooperative Ramp Merging in Mixed Traffic Environments [J]. IEEE Intelligent Transportation Systems Magazine, 2022,14(6):52.

[18] KESTING A, TREIBER M, HELBING D. General lane-changing model mobil for car-following models [J]. Transportation Research Record, 2007,1999(1): 86.

[19] TREIBER M, HENNECKE A, HELBING D. Congested traffic states in empirical observations and microscopic simulations [J]. Physical Review E, 2000,62(2): 1805.

[20] SALVUCCI D D, LIU A. The time course of a lane change: driver control and eye-movement behavior [J]. Transportation Research Part F: Traffic Psychology and Behaviour, 2002, 5 (2): 123.

[21] KESTING A, TREIBER M, SCHÖNHOF M, *et al*. Adaptive cruise control design for active congestion avoidance [J]. Transportation Research Part C: Emerging Technologies, 2008,16(6): 668.

[22] ZHENG Y, RAN B, QU X, *et al*. Cooperative lane changing strategies to improve traffic operation and safety nearby freeway off-ramps in a connected and automated vehicles environment [J]. IEEE Transactions on Intelligent Transportation Systems, 2019,21(11): 4605.

[23] ZHENG Y, ZHANG G, LI Y, *et al*. Optimal jam-absorption driving strategy for mitigating rear-end collision risks with oscillations on freeway straight segments [J]. Accident Analysis & Prevention, 2020,135: 105367.

[24] ALIWA E, RANA O, PERERA C, *et al*. Cyberattacks and countermeasures for in-vehicle networks [J]. ACM Computing Surveys, 2021,54(1): 1.

[25] WANG P, WU X, HE X. Modeling and analyzing cyberattack effects on connected automated vehicular platoons [J]. Transportation Research Part C: Emerging Technologies, 2020,115: 102625.

[26] ZHANG T, YE D. False data injection attacks with complete stealthiness in cyber - physical systems: a self-generated approach [J]. Automatica, 2020,120: 109117.