Physica A 496 (2018) 351–370

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

An extended car-following model to describe connected traffic dynamics under cyberattacks

Pengcheng Wang, Guizhen Yu, Xinkai Wu *, Hongmao Qin, Yunpeng Wang

School of Transportation Science and Engineering, Beijing Key Laboratory for Cooperative Vehicle Infrastructure Systems and Safety Control, Beihang University, Beijing 100191, China

HIGHLIGHTS

- The impacts of the potential cyberattacks on vehicles are modeled.
- The linear and nonlinear stability analysis are conducted respectively.
- Our model can avoid collisions and relieve traffic congestion with cyberattacks.

ARTICLE INFO

Article history:
Received 18 July 2017
Received in revised form 24 October 2017
Available online 27 December 2017

Keywords:
Car-following
Cyberattacks
Linear stability theory
Reductive perturbation method

ABSTRACT

In this paper, the impacts of the potential cyberattacks on vehicles are modeled through an extended car-following model. To better understand the mechanism of traffic disturbance under cyberattacks, the linear and nonlinear stability analysis are conducted respectively. Particularly, linear stability analysis is performed to obtain different neutral stability conditions with various parameters; and nonlinear stability analysis is carried out by using reductive perturbation method to derive the soliton solution of the modified Korteweg de Vries equation (mKdV) near the critical point, which is used to draw coexisting stability lines. Furthermore, by applying linear and nonlinear stability analysis, traffic flow state can be divided into three states, i.e., stable, metastable and unstable states which are useful to describe shockwave dynamics and driving behaviors under cyberattacks. The theoretical results show that the proposed car-following model is capable of successfully describing the car-following behavior of connected vehicles with cyberattacks. Finally, numerical simulation using real values has confirmed the validity of theoretical analysis. The results further demonstrate our model can be used to help avoid collisions and relieve traffic congestion with cybersecurity threats.

1. Introduction

With the growing number of vehicles in our daily life, traffic congestions and accidents are becoming extremely serious issues [1–3]. In this context, connected vehicle technology, one necessary component of Intelligent Transportation Systems (ITS), is considered as a highly promising solution to significantly improve transport mode in the foreseeable future [4,5]. Through employing the wireless communication, driving information such as speed, position, inter-vehicle distance, etc. can be shared and exchanged. By this way, connected vehicle technology can enhance traffic safety and road capacity. But due to the vulnerability of vehicular networks, connected vehicles can be controlled unlawfully by infiltrating malicious messages.

* Corresponding author.
E-mail address: xinkaiwu@buaa.edu.cn (X. Wu).

https://doi.org/10.1016/j.physa.2017.12.013
0378-4371/

The violation of cybersecurity may result in serious issues such as traffic congestion and even collisions. Therefore, more and more scholars and automotive engineers have begun to research cyberattacks on vehicles [6–10].

To date, there is limited literature about the impact of malicious attacks on connected vehicles, particularly the driving behaviors in traffic road with cyberattacks. For instance, Reilly et al. [11] studied the impact of attacks on traffic control systems in a macroscopic level; Amoozadeh et al. [12] considered the effects of security attacks on the connected vehicles by using VEhicular NeTwork Open Simulator (VENTOS); Dadras et al. [13] argued that the vehicle platoon turns unstable when an cybersecurity attack appears; Gerdes et al. [14] found that the efficiency attack could degrade the performance of automated transportation systems. These studies demonstrate that cyberattacks could significantly deteriorate traffic conditions, leading to a serious congestion and even accidents. However, the existing models or methods have not clearly explained vehicles' behaviors under cybersecurity threats. To better understand these complex impacts, it is necessary to develop a sophisticate traffic flow model.

In general, traffic flow can be divided into macroscopic and microscopic models [15–19]. The former aims to describe overall behavior of road vehicles such as flow, mean speed and density; while the latter, especially car-following models can describe traffic dynamics at a higher detailed level like the movement of individual cars and interactions between two successive cars. For our purpose, the car-following models are selected to characterize the dynamic change of connected vehicles with cyberattacks.

The car-following model is first proposed by Reuschel [20] and Pipes [21]. Following their work, a great deal of extended car-following models from early Gazis–Herman–Rothery (GHR) models [20–23], collision-avoidance models [24–27], Helly's linear model [28–30], to recent Cellular Automata (CA) [31–33], action-point (AP) or psychophysical models [34–36], fuzzy-logic model [37–40], and optimal velocity (OV) model [41–46] were developed to address various issues. Some of these models were developed to investigate car-following behaviors of connected vehicles [47–50]. For instance, Monteil et al. [51] used a general car-following form to analyze cooperative driving model; Yu and Shi [52] evaluated the impacts of relative velocity fluctuation on traffic dynamics and fuel consumptions; Kesting et al. [53] considered the impacts of vehicles equipped with adaptive cruise control (ACC) on driving behavior; Peng et al. [54] considered the effect of the optimal changes with memory using a full velocity difference model; Ngoduy [55] investigated the effect of intelligent vehicles on heterogeneous traffic flow instabilities from a small disturbance; Li et al. [56] extended the full velocity difference model (FVD) by incorporating electronic throttle opening angle to better describe the characteristics of connected vehicles; and Tang et al. [57] analyzed the traffic behavior with consideration of inter-vehicle communication (IVC) under accidents. In spite of many car-following models have been developed, however, to best of our knowledge, very few studies on the impacts of the emerging cyberattacks on vehicles have been conducted.

Therefore, to better study traffic behaviors under security threats for connected vehicles, an improved car-following model is presented here extended from original optimal velocity (OV) model [42]. The OV model is sententious and intuitive to describe following behavior, as mentioned in [58]. Increasing number of scholars are interested in this model [59–64]. Our goal is to describe traffic dynamics with the potential cyberattacks. To this end, we first extend the OV model by introducing two additional weight parameters to characterize different security attacks. Then, linear and nonlinear stability analysis of the proposed model are preformed to investigate the evolution of traffic flow impacted by cyberattacks. Numerical simulations are used to validate the theoretical analysis and illustrate the fluctuation behavior of traffic flow under attacks. Furthermore, theoretical and numerical results illustrate that the proposed model could be applied to assist drivers to avoid crash and relieve traffic jam.

The remainder of this paper is organized as follows. Section 2 presents an extended car-following model. Sections 3 and 4 present the linear and nonlinear stability analysis, respectively. In Section 5, numerical simulation is conducted to illustrate the impacts of attacks on connected vehicles. Section 6 concludes this paper and discusses the future research.

2. An extended car-following model for cyberattacks

Connected vehicles can perceive nearby vehicles' intentions and surrounding environment through wireless communication and advanced on-board sensors. Since vehicles' internal networking and its connection to external networks opens doors to malicious attacks, lots of reports demonstrates that various attacks could cause serious problems such as congestion, privacy disclosure and even car crash [65–67]. Some well-known cyberattacks like *Denial of Service* (DoS), *Bogus information*, *spoofing*, *replay* and *suppression* are briefly summarized as follows:

(1) DoS: This attack could cause network communication interruption. Once access to communication network like VANETs has been granted, attackers could inject unnecessary data into the nodes (i.e., vehicles and infrastructure) and jam the network. Generally, DoS attacks can interfere or suppress the communication between vehicles. If one car is corroded by DoS attacks in a connected vehicle stream, the whole stream could be collapsed due to the spread of infection.

(2) *Falsification*: An attacker can modify the information and send false messages, and the erroneous messages tempered will be further sent to neighbor nodes, thereby confusing drivers. This cyberattack could also cause serious traffic problems in network. For example, in a connected vehicle platoon, if bogus velocity messages are sent to following vehicles, the traffic flow will become unstable leading unnecessary traffic delay or even severe collisions.

(3) *Spoofing*/*masquerading*: An attacker could pretend to be another certain authorized vehicle and aims to take over other vehicles' legal identities. Once attackers successfully falsify other vehicles' identities, they will gain the legitimate access of these vehicles and broadcast fraudulent information to other target vehicles. Similar to falsification attacks, *spoofing* also broadcasts false beacon messages; but *spoofing* is more severe since it has the authorized access.

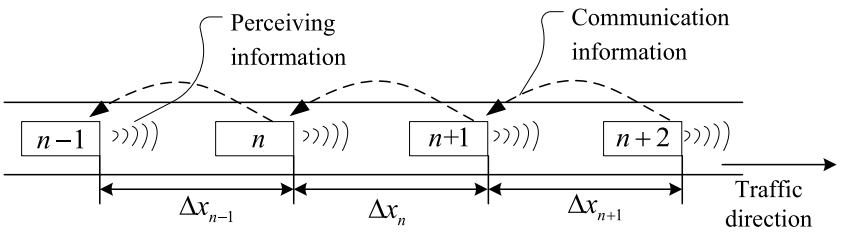


Fig. 1. An illustration of connected vehicles. $\Delta x_n = x_{n+1} - x_n$ indicates the space headway between car n and car $(n+1)$, where x_n denotes the position of car n.

(4) *Replay/delay* and *suppression*: As the name shows, this type of attack first listens and stores messages, and replays the messages to the target vehicle(s) at a later time. Due to the delay, the valid messages become useless. More importantly, such repeated and delayed message could potentially disturb the traffic and cause malfunctions for real-time applications. For instance, if the warning message of the upfront road maintenance is suppressed or delayed, the vehicles could not receive this message, causing a pile-up effect and even collisions.

All the aforementioned security attacks will lead to the change of driving behaviors, particularly the car following behavior. This paper aims to develop a car-following model that can reflect the changes caused by cyberattacks. To highlight the key concepts of our model, we put forward the following assumptions: (1) the connected vehicles group as a platoon and travel on a straight single-lane highway; (2) all following vehicles update their dynamical parameters autonomously in the light of the speed and position changes of the leading car; (3) the connected vehicles adopt a simple look-ahead-to-the-direct-leader communication protocol [12], i.e., the following car only receives beacon messages from its directly preceding car (see Fig. 1). Note, to simplify the modeling and emphasize the effects of cyberattacks, we use a relatively simple look-ahead-to-the-direct-leader protocol in the connected vehicles. But such a protocol is a reasonable communication way to reveal traffic dynamics with cyberattacks as presented in [12,68,69]. Further extension to more complicated communication topologies will be studied in our future work.

The general form of time-continuous car-following model is provided in Eq. (1), which formulates the basic principle of following behavior, i.e., response to stimulus [70]:

$$\ddot{x}_n = f_{sti}(v_n, \Delta x_n, \Delta v_n), \tag{1}$$

where $\ddot{x}_n$ represents the acceleration of car n; f_{sti} is the stimulus function; $\Delta x_n = x_{n+1} - x_n$ denotes the space headway between the car n and car $(n+1)$, here x_n is the position of car n; $\Delta v_n(t) = v_{n+1}(t) - v_n(t)$ represents the velocity difference between the consecutive cars, here $v_n(t)$ is the speed of car n. Note different car-following models have different f_{sti} by taking into account varying stimulus derived from drivers, sensors and communication [71–76].

To derive the explicit stimulus function of Eq. (1), a widely recommended stimulus function proposed by Newell [23] and Whitham [77] is presented as follows:

$$\frac{\mathrm{d}x_n(t+\tau)}{\mathrm{d}t} = V\left(\Delta x_n(t)\right), \tag{2}$$

where $x_n(t)$ is the position of car n at time t, $V(\Delta x_n(t))$ is the optimal velocity function with respect to the space headway, and τ is a delay time. This model essentially reveals that a driver could alter the current velocity to an optimal one dependent on the headway with a delay time τ.

We would like to point out that many other scholars also applied the OV model to describe different traffic environments due to its simplicity, intuitiveness, and innovativeness. For example, Hasebe et al. [62] used an extended OV model to consider multiple cars ahead; Zhou et al. [64] studied the optimal velocity difference model with the reaction-time delay of drivers; and Nagatani [78] extended the OV model to investigate the next-nearest-neighbor interaction. Although it has some shortcomings such as jump in speeds, infinite acceleration and jerk, we believe such a simply model is competent to reveal the essential of traffic flow under cyberattacks.

It is clear that connected vehicles equipped with V2X can receive dynamic information including speed, acceleration, headway, etc. from the preceding cars, allowing each car to predict acceleration requirement to keep smaller safe inter-vehicle gap than manual driving mode. If without any influence of cyberattacks, dynamic information will be accurately send to the following vehicle on time. However, if connected vehicles are influenced by cyberattacks, the information transmission between vehicles could be interrupted, delayed, lost, or even falsified. These attacks, in essence, can alter the size of velocity difference and distance difference of between successive cars, in which the size of velocity difference denotes the size of velocity difference between successive cars. For instance, if one attacker tampers the subject car's velocity, then the velocity difference between the subject car and its preceding car will be changed.

Hence, when considering security threats on vehicles, Eq. (2) can be rewritten as the following structure:

$$\frac{\mathrm{d}x_n(t+\tau)}{\mathrm{d}t} = V\left(\gamma \Delta x_n(t), q\Delta v_n(t)\right), \tag{3}$$

where γ, q are the weight parameters which can describe the impacts of cyberattacks on headway and velocity difference between consecutive cars, respectively.

Note that different values of γ and q can respectively alter the values of headway and relatively velocity, thereby quantifying the impacts of cyberattacks on vehicles. Indeed, the exact projections between the values of γ, q and different threats are still unknown, and might be very difficult to be found out. In this paper, we focus on showing the impacts of potential cyberattacks on connected vehicles by altering the values of γ and q.

As stated by [61,79,80], the optimal velocity function with multi-parameters can be linearized by adding adjustable weights. Hence, Eq. (3) can be expanded as follows:

$$\frac{\mathrm{d}x_n(t+\tau)}{\mathrm{d}t} = V\left(\gamma \Delta x_n(t)\right) + \lambda q \Delta v_n(t), \tag{4}$$

where λ is the response coefficient of the altered relative velocity $q\Delta v_n(t)$.

Eq. (4) can be further elaborated using the explicit optimal velocity expression proposed by Bando [42]:

$$V\left(\Delta x_n\right) = \frac{v_{\max}}{2}\left[\tanh\left(\Delta x_n - h_c\right) + \tanh\left(h_c\right)\right], \tag{5}$$

where h_c is the safety distance and $v_{\max}$ is the maximal velocity.

Note that Eq. (5) is a monotonically increasing function with an upper bound because the first derivative of $V(\Delta x_n)$, i.e., $V'(\Delta x_n) = v_{\max}[1 - \tanh^2(\Delta x_n - h_c)]/2$ is nonnegative for arbitrary value of Δx_n; and the value of $V(\Delta x_n)$ is not more than $v_{\max}$. Besides, Eq. (5) has an inflection point at $\Delta x_n = h_c$ since the second order of $V(h_c)$ is equal to 0, i.e., $V''(h_c) = [\mathrm{d}^2V(\Delta x_n)/\mathrm{d}(\Delta x_n)^2]_{\Delta x_n = h_c} = 0$, which is a necessary factor to address the nonlinear stability in later paper. Indeed, Eq. (5) can describe basic car-following behaviors, i.e., if the inter-vehicle distance is less than the safety distance, the driver will reduce vehicle speed to avoid rear-end collision; otherwise, the following vehicle will travel with a higher velocity.

Therefore, $V\left(\gamma \Delta x_n(t)\right)$ can be converted to a format of $weight \times V\left(\Delta x_n(t)\right)$ due to its monotonicity. Hence, Eq. (4) can be rewritten as:

$$\frac{\mathrm{d}x_n(t+\tau)}{\mathrm{d}t} = pV\left(\Delta x_n(t)\right) + \lambda q \Delta v_n(t), \tag{6}$$

where p is a weight to adjust $V\left(\Delta x_n(t)\right)$ to be equivalent to $V\left(\gamma \Delta x_n(t)\right)$. Note Eq. (6) essentially transfers the direct influence of attacks on inter-vehicle distance to the influence on optimal velocity.

By employing Taylor expansion, Eq. (6) can be expanded to the following equation:

$$\frac{\mathrm{d}^2x_n(t)}{\mathrm{d}t^2} = \alpha\left[pV\left(\Delta x_n(t)\right) - \frac{\mathrm{d}x_n(t)}{\mathrm{d}t}\right] + kq\Delta v_n(t), \tag{7}$$

where $\alpha = 1/\tau$ is a driver's sensitivity coefficient that represents the intension level of the driver responding to stimulus, and $k = \lambda/\tau$.

Note that the derived Eq. (7) becomes an optimal velocity model without explicit delay after removing higher order of the Taylor expansion. As suggested by [79,81,82], removing higher order of the Taylor expansion is a common way in car-following modeling. The main reason is that keeping the higher order of the Taylor expansion will make the rest of mathematical modeling too complicated. Also, the higher order of the Taylor expansion is relatively small; so, to some extent, Eq. (7) is approximately equal to Eq. (6) and we believe that this is a reasonable way in our modeling.

In addition, although our model is similar to the FVD model proposed by Jiang [83] from the view of the equation structure, they are designed to serve different purposes. From the perspective of physical meaning, our model aims to address the traffic flow patterns under cyberattacks, while the FVD model is to describe general traffic flow behaviors without cybersecurity threats. Furthermore, our model has different mathematical expression from the FVD model. The proposed model Eq. (7) is derived from a classical OV model through precise mathematical discussion. For some special cases, it can be described by the FVD model from the general parameter perspective. But our model is specifically designed for characterizing the traffic flow behavior with cybersecurity threats, while the general FVD model cannot directly describe the effect of cyberattacks on vehicles such as bogus information, replay attack and suppression.

In fact, p, q that are used to characterize the impact of security threats on driving behaviors have clear physical meanings. If $p = q = 1$, it indicates the connected vehicles are moving without cyberattacks, and Eq. (7) will be converted into a classical car-following model as proposed by Xue [61]. When $p \neq 1$ and/or $q \neq 1$, it denotes the connected vehicles are influenced by cyberattacks. Particularly, if $p > 1$, it shows that the cyberattacks "forge" or "falsify" messages which lure the following drivers to perceive an overestimated headway compared to the real one. This wrong message could cause the following drivers to make the wrong decision of acceleration in order to reduce the "false" large gap and lead to potential collisions. On the other hand, if $p < 1$, the cyberattacks "forge" messages to lure the following drivers to perceive an underestimated headway, which could cause the following drivers to make the wrong decision of deceleration in order to maintain a safe gap and lead to unnecessary delay. Similarly, if $q > 1$, the cyberattacks create wrong messages which might lure the following drivers to believe the velocity difference between vehicles is high and cause the drivers to make the wrong decision of acceleration; and if $q < 1$, drivers could make the wrong decision of deceleration leading unnecessary delay due to the wrong information of velocity difference.

For the convenience of numerical computation, as pointing by Nagatani [44,78,84], Eq. (7) can be transformed into the following difference formation with regard to the time by using the asymmetric forward difference [78]:

$$\begin{aligned} & x_n(t+2\tau) - x_n(t+\tau) \\ = \; & \tau p V\left(\Delta x_n(t)\right) + \lambda q \left(x_{n+1}(t+\tau) - x_n(t+\tau) - x_{n+1}(t) + x_n(t)\right). \end{aligned} \tag{8}$$

For the sake of the linear and nonlinear stability analysis in later paper, Eq. (8) can be further rewritten as:

$$\begin{aligned} & \Delta x_n(t+2\tau) - \Delta x_n(t+\tau) \\ = \; & \tau p \left[V\left(\Delta x_{n+1}(t)\right) - V\left(\Delta x_n(t)\right)\right] \\ & + \lambda q \left(\Delta x_{n+1}(t+\tau) - \Delta x_n(t+\tau) - \Delta x_{n+1}(t) + \Delta x_n(t)\right). \end{aligned} \tag{9}$$

3. Linear stability analysis

In this section, the stability of the proposed model is analyzed by using a linear stability theory [85–88]. We assume that a connected vehicles platoon is moving on a single lane with no lane changing and no overtaking. The solution of the uniformly steady state of Eq. (8) is given by:

$$x_n^0(t) = hn + V(h)t, \qquad \text{with} \quad h = L/N, \tag{10}$$

where h indicates the constant inter-vehicle distance, N is the number of vehicles in the observed lane, and L is the road length.

By introducing a small deviation $y_n(t)$ to the uniform steady state Eq. (10), an updated position solution is obtained:

$$x_n(t) = x_n^{(0)}(t) + y_n(t). \tag{11}$$

Submitting Eq. (11) into Eqs. (10), (9) can be further rewritten as:

$$\begin{aligned} & \Delta y_n(t+2\tau) - \Delta y_n(t+\tau) \\ = \; & \tau p V'\left(\Delta y_{n+1}(t) - \Delta y_n(t)\right) \\ & + \lambda q \left[\Delta y_{n+1}(t+\tau) - \Delta y_{n+1}(t) - \Delta y_n(t+\tau) - \Delta y_n(t)\right], \end{aligned} \tag{12}$$

where $V' = V'(h)$ is the derivative of $V(\Delta x_n(t))$ at $\Delta x_n(t) = h$, and $\Delta y_n(t) = y_{n+1}(t) - y_n(t)$.

The small perturbation can be expanded as the following Fourier mode [51,89]:

$$\Delta y_n(t) = A e^{ikn - i\omega t}, \tag{13}$$

where k is the wavenumber ($0 \le k \le \pi$), n is the car' serial number, and ω is the wave angular frequency.

Next, we set $z = -i\omega$, then Eq. (12) can be rewritten as:

$$e^{2z\tau} - e^{z\tau} = \tau p V' \left(e^{ik} - 1\right) + \lambda q \left(e^{ik + z\tau} - e^{ik} - e^{z\tau} + 1\right). \tag{14}$$

For an exponential function in Eq. (14), z can be regarded as the order of ik. Hence, z is expanded as $z = z_1(ik) + z_2(ik)^2 + \cdots$ with the long wave modes [90]. Submitting it into Eq. (14), we can get the first- and second-order of ik as below:

$$\begin{aligned} z_1 &= pV', \\ z_2 &= -\frac{3}{2} z_1^2 \tau + \frac{pV'}{2} + \lambda q z_1. \end{aligned} \tag{15}$$

For long-wavelength modes, if z_2 is negative, the uniform steady flow will lose the original stability; if z_2 is positive, the traffic flow keeps the steady state. $z_2 = 0$ indicates the neutral stability condition or critical condition which is written by

$$\tau_c = \frac{1 + 2\lambda q}{3pV'}. \tag{16}$$

Hence, the unstable and stable condition can be indicated by $\tau > \tau_c$ and $\tau < \tau_c$, respectively. From Eq. (5), the derivate of the optimal velocity function has a constant value at $\Delta x_n = h_c$ independent of time, i.e., $V'(h_c) = v_{\max}/2$. Therefore, Eq. (16) can be further simplified as follows:

$$\tau_c = \frac{2 + 4\lambda q}{3p v_{\max}}. \tag{17}$$

Note, the inverse of critical delay time, i.e., $\alpha_c = 1/\tau_c$ is also called the critical sensitivity. If $\alpha > \alpha_c$, the uniform steady stream keeps stable regardless of traffic density (i.e., headway); otherwise, if $\alpha < \alpha_c$, the stability of the traffic flow is dependent on the traffic density.

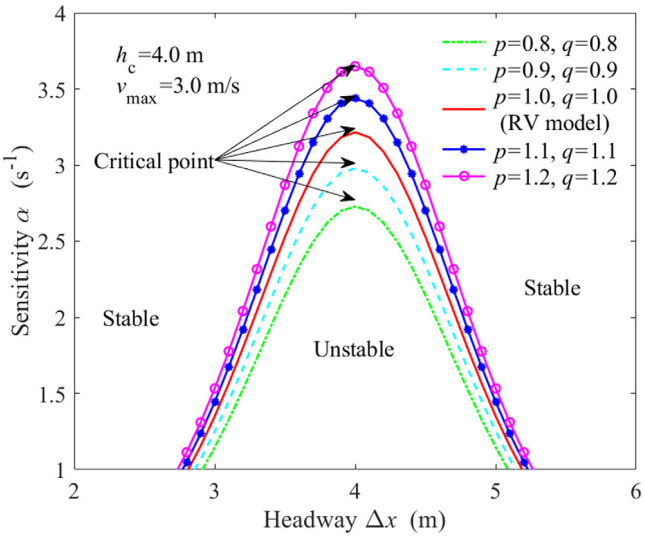


Fig. 2. Neutral stability lines with different parameter sets $(p,\ q)$. The green dot line corresponds to $p = 0.8,\ q = 0.8$; the light blue dash line corresponds to $p = 0.9,\ q = 0.9$; the red solid line corresponds to $p = 1,\ q = 1$, i.e., RV model; the blue asterisk line corresponds to $p = 1.1,\ q = 1.1$; and the magenta circle line corresponds to $p = 1.2,\ q = 1.2$, where $\lambda = 0.2$. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Furthermore, we would like to point out that this paper adopts the long-wavelength stability analysis, instead of the short-wavelength stability analysis [91] since this method has been widely used in many publications for both macroscopic and microscopic models [92]. It has been argued that applying different wavelength stability analyses could generate different stable conditions [93]. Indeed, it is true that the "stable" traffic under the long-wavelength stability condition may still unstable under the short-wavelength stability condition. For instance, Berg et al. [94] claimed that the macroscopic hydrodynamic model has an instability, which is resulted from short-wavelength fluctuations. But such instability is not presenting in the classical car-following model. However, if the short-wavelength fluctuations are properly regularized as suggested by [95], such instability could disappear.

Moreover, from the view of pure mathematics, our proposed model has a good compatibility and interoperability for many typical car-following models. For instance, if $p = q = 1$, the stability condition for Eq. (16) is degraded to the relative velocity (RV) model proposed by Xue [61].

In Fig. 2, the red solid line corresponds to $p = 1,\ q = 1$ which is equivalent to the RV model proposed by Xue [61]. As shown in this figure, four lines associated with the considered model are plotted to describe the stability of the traffic stream with cyberattacks. The apex of each line denotes the critical point. Each line separates stable and unstable regions for traffic flow. Note that different weights of $p,\ q$ can generate different stable region, i.e., various cyberattacks may cause varying traffic oscillation behavior. Here, to further explore the driving behavior influenced by cyberattacks, we use the stability condition of the RV model (i.e., the red solid line) without cyberattacks as a benchmark, to compare with the evolution of traffic flow under different cyberattacks.

Moreover, $p \neq 1$ and/or $q \neq 1$ indicate that the traffic stream is infected by cyberattacks. Fig. 2 shows that the stable region increases with the decrease of p and q values. In detail, larger parameters (i.e., $p > 1,\ q > 1$) indicate that cyberattacks create wrong impressions of bigger headways and larger velocity differences to drivers. With such illusion, drivers are very likely to speed up in order to reduce the gap between other vehicles; this could lead to severe rear-end collisions and the paralysis of the whole traffic. On the other hand, smaller $p,\ q$ values could lead to more stable traffic due to larger stable region as shown in the figure. The reason is that the wrong impressions of smaller headways and reducing velocity differences generated by cyberattacks actually could allure drivers to slow down. By doing so, in some sense, driving behavior actually becomes safer thereby enlarging the stable region. But we have to point out that although some attacks may improve the stability of traffic but at the cost of more delay due to unnecessary slowing down caused by wrong leading information. We call this type of stability as the "unhealthy" stability inspirited from ill-conditioned equation. Such "unhealthy" stability will make traffic state more stable but not optimal, compared to RV, due to declined roadway capacity and increased unnecessary delay. Therefore, the performance of the whole system has been downgraded.

To further explore how p or q impacts the traffic flow, Figs. 3 and 4 are plotted. Fig. 3 presents the change of headway-sensitivity with different p when $q = 1$, while Fig. 4 shows the change of headway-sensitivity with varying q when $p = 1$. For both figures, with the increase of p or q, the area of stable region decreases. Importantly, for the same increment, the headway (Δx_n) brings greater impact on traffic flow than velocity difference (Δv_n) does. This clearly indicates that wrong message of inter-vehicle gap may cause more serious traffic problem comparing with wrong information of relative velocity.

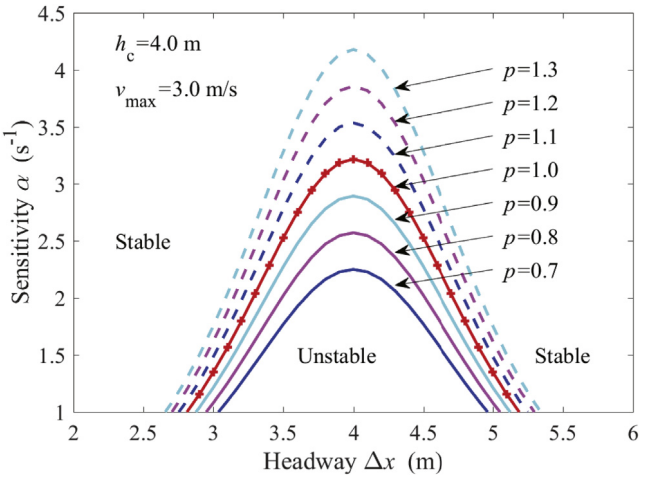


Fig. 3. Neutral stability lines of headway-sensitivity with different p when $q = 1$.

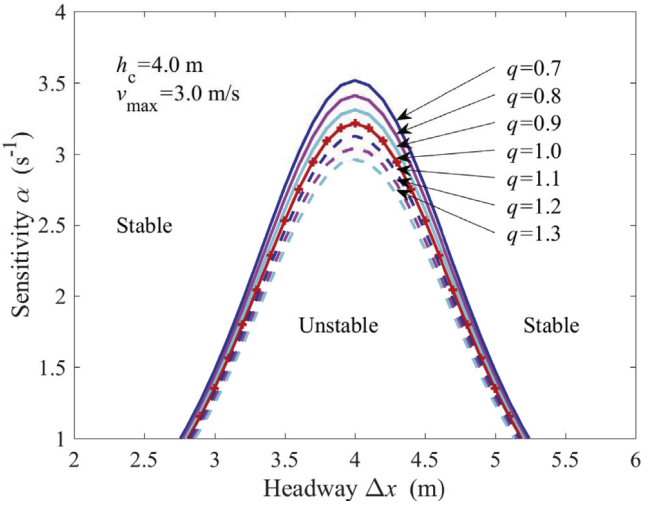


Fig. 4. Neutral stability lines of headway-sensitivity with different q when $p = 1$.

4. Nonlinear stability analysis

In this section, we apply the reductive perturbation method [96–98] to investigate the nonlinear stability of our model. This analysis, based on the coarse-grained scales for long-wavelength models, can derive the solution of the mKdV equation that is applied to characterize the kink density wave. By introducing slow scales for space variable n and time variable t, we can further investigate the slow varying behavior near the critical point (h_c, α_c) [58]. Then the corresponding slow variables X and T are defined as below:

$$X = \varepsilon(j + bt), \quad T = \varepsilon^3 t, \quad 0 < \varepsilon \ll 1, \tag{18}$$

where b is to-be-determined constant. Adding a small fluctuation function $\varepsilon R(X, T)$ with respect to space variable X and time variable T, the headway can be followed by:

$$\Delta x_n(t) = h_c + \varepsilon R(X, T). \tag{19}$$

With the help of Eqs. (18) and (19), we expand Eq. (9) to the fifth order of ε and obtain the following partial differential equation:

$$\begin{aligned}&\varepsilon^2\left(b-pV'\right)\partial_X R+\varepsilon^3\left[\frac{3b^2\tau}{2}-\frac{pV'}{2}-\lambda qb\right]\partial_X^2 R\\&+\varepsilon^4\left\{\partial_T R+\left[\frac{7b^3\tau^2}{6}-\frac{pV'}{6}-\lambda q\frac{b+b^2\tau}{2}\right]\partial_X^3 R-\frac{pV'''}{6}\partial_X R^3\right\}\\&+\varepsilon^5\left\{(3b\tau-\lambda q)\,\partial_X\partial_T R+\left[\frac{5b^4\tau^3}{8}-\frac{pV'}{24}-\lambda q\cdot\frac{2b+3b^2\tau+2b^3\tau^2}{12}\right]\partial_X^4 R-\frac{pV'''}{12}\partial_X^2 R^3\right\}=0,\end{aligned}\tag{20}$$

where V', V''' are the first- and third-derivative of $V(\Delta x_n)$ at $\Delta x_n = h_c$, respectively.

By taking $b = pV'$ and $\tau = (1+\varepsilon^2)\tau_c$ near the critical point (h_c, α_c), the second- and third-order of ε will be eliminated from Eq. (20). Then Eq. (20) can be written as below:

$$\varepsilon^4\left\{\partial_T R-g_1\partial_X^3 R+g_2\partial_X R^3\right\}+\varepsilon^5\left\{g_3\partial_X^2 R+g_4\partial_X^2 R^3+g_5\partial_X^4 R\right\}=0,\tag{21}$$

where $g_1 = \frac{pV'}{6}+\frac{\lambda q(b+b^2\tau_c)}{2}-\frac{7b^3\tau_c^2}{6}$, $g_2 = -\frac{pV'''}{6}$, $g_3 = \frac{3b^2\tau_c}{2}$, $g_4 = \frac{6b\tau_c-2\lambda q-1}{12}V'''$, $g_5 = -\frac{23b^4\tau_c^3}{8}+\frac{pV'(12b\tau_c-4\lambda-1)}{24}+\frac{\lambda q(30b^3\tau_c^2+15b^2\tau_c-2b)}{12}-\frac{\lambda^2q^2(b+b^2\tau_c)}{2}$.

In order to obtain the regularized equation, we introduce the transformations $T = T'/g_1$ and $R = R'\sqrt{g_1/g_2}$ into Eq. (21), then we can obtain

$$\partial_{T'}R'-\partial_X^3 R'+\partial_X R'^3+\varepsilon\left(\frac{g_3}{g_1}\partial_X^2 R'+\frac{g_4}{g_2}\partial_X^2 R'^3+\frac{g_5}{g_1}\partial_X^4 R'\right)=0.\tag{22}$$

Omitting the $O(\varepsilon)$ term in Eq. (22), we get the mKdV equation with a kink solution that is regarded as a desired solution:

$$R'_0\left(X,T'\right)=\sqrt{c}\tanh\sqrt{\frac{c}{2}}\left(X-cT'\right),\tag{23}$$

where c is a propagation velocity of the kink–antikink soliton solution and c is determined by the $O(\varepsilon)$ term.

Next, we suppose $R'(X,T') = R'_0(X,T') + \varepsilon R'_1(X,T')$ and consider the $O(\varepsilon)$ correction. It is necessary to satisfy the following solvability condition to obtain the value of propagation velocity c [99,100].

$$\left(R'_0, M[R'_0]\right)=\int_{-\infty}^{\infty}\mathrm{d}X R'_0\left(X,T'\right)M\left[R'_0\left(X,T'\right)\right]=0,\tag{24}$$

where $M[R'_0] = M[R']$, $M[R'] = \frac{g_3}{g_1}\partial_X^2 R'+\frac{g_4}{g_2}\partial_X^2 R'^3+\frac{g_5}{g_1}\partial_X^4 R'$.

By integrating Eq. (24), the propagation velocity c is given by:

$$c=\frac{5g_2g_3}{2g_2g_5-3g_1g_4}.\tag{25}$$

Hence, the solution of Eq. (21) is obtained as follows:

$$R\left(X,T\right)=\sqrt{\frac{g_1c}{g_2}}\cdot\tanh\sqrt{\frac{c}{2}}\left(X-cg_1T\right).\tag{26}$$

From Eq. (5), we know that $V' = v_{\max}/2$, $V''' = -v_{\max}$ at $\Delta x_n = h_c$ irrespective of time change. Thus, the amplitude A of the kink soliton is given by:

$$A=\left[\frac{g_1c}{g_2}\left(\frac{\alpha_c}{\alpha}-1\right)\right]^{1/2}\quad\text{with}\quad\alpha_c=\frac{3pv_{\max}}{4\lambda q+2}.\tag{27}$$

Therefore, the kink–antikink density wave soliton solution of the headway is given by:

$$\Delta x_n(t)=h_c+\sqrt{\frac{g_1c}{g_2}\left(\frac{\alpha_c}{\alpha}-1\right)}\tanh\left\{\sqrt{\frac{c}{2}\left(\frac{\alpha_c}{2}-1\right)}\cdot\left[n+\left(1-cg_1\left(\frac{\alpha_c}{\alpha}-1\right)\right)t\right]\right\}.\tag{28}$$

Applying the results of nonlinear stability analysis, Fig. 5 shows a more detailed phase space of the headway and sensitivity compare with Fig. 2. In Fig. 5, the dotted lines and solid lines are respectively derived from the coexisting conditions and neutral stability conditions. Indeed, the coexisting curves are plotted via the solution of the mKdV equation. For each pair of $(p,\ q)$ in this figure, the coexisting and neutral stability curves divide the whole region into three parts: the region outside the coexisting curve represents that traffic flow is stable, the region inside the neutral stability curve denotes that traffic flow is unstable, and the region between the coexisting and neutral stability curves represents that traffic flow is metastable. The coexisting phase, also called metastable state, indicates a combination of freely moving phase with low

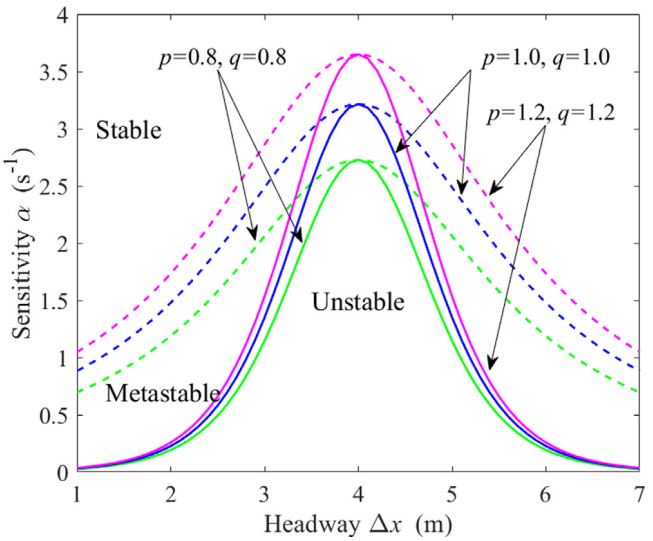


Fig. 5. Phase space of the headway-sensitivity with stable, metastable and unstable states.

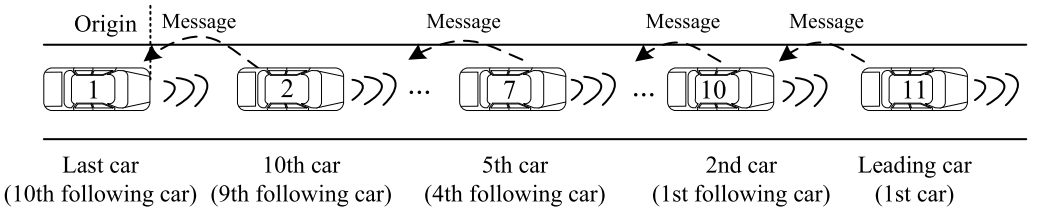


Fig. 6. Schematic diagram of initial conditions for the connected vehicles.

density and jam phase with high density. More specifically, the headways in free flow state and in traffic congested state are respectively indicates by $\Delta x_n = h_c + A$ and $\Delta x_n = h_c - A$, which are used to obtain the coexisting phase.

5. Simulation

The stability analysis in the last sections demonstrated some correlations between cyberattacks and traffic oscillation. In this section, we will more directly address those correlations from the point of view of individual vehicles' behaviors using our new model through numerical simulations.

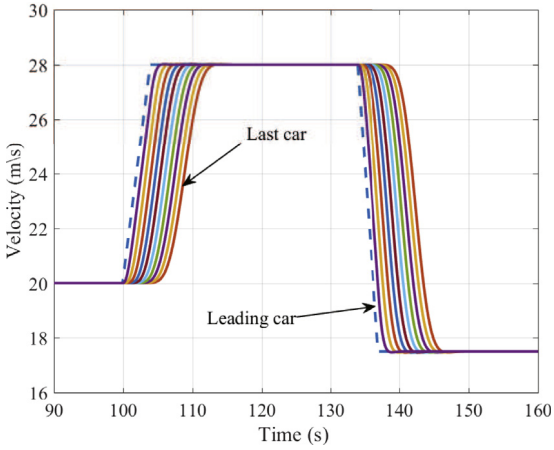
As shown in Figs. 2–5, Eq. (5) only adopts small parameters' value due to its limitation. Hence, To better simulate actual traffic phenomenon, we adopt another optimal velocity function [64,101,102] instead of Eq. (5). This new-introduced OV function is derived from a sigmoidal function $V(\Delta x) = 16.8[\tanh 0.086(\Delta x - 25) + 0.913]$ that uses the practical observed data from Japanese freeway; obviously, it represents more realistic traffic phenomena compared to other OV functions. Please refer to the literature [103–105] for more details.

$$V^{\mathrm{op}}\left(\Delta x_n(t)\right) = \frac{v_{\max}}{2}\left[1 + H\left(2 \cdot \frac{\Delta x_n(t) - \eta}{\xi}\right)\right], \tag{29}$$

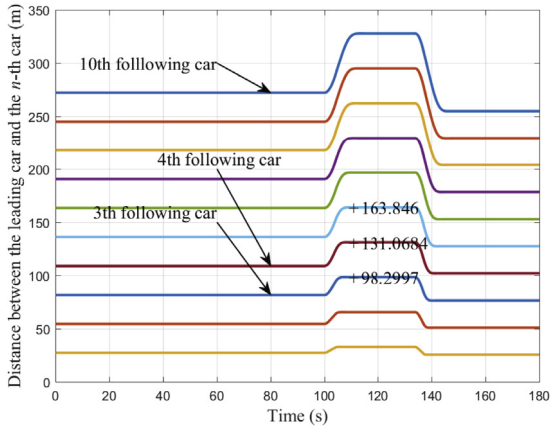
where the saturation function $H(\rho)$ is described as

$$H(\rho) = \begin{cases} 1, & \rho > 1; \\ \rho, & -1 \le \rho \le 1; \\ -1, & \rho < -1. \end{cases}$$

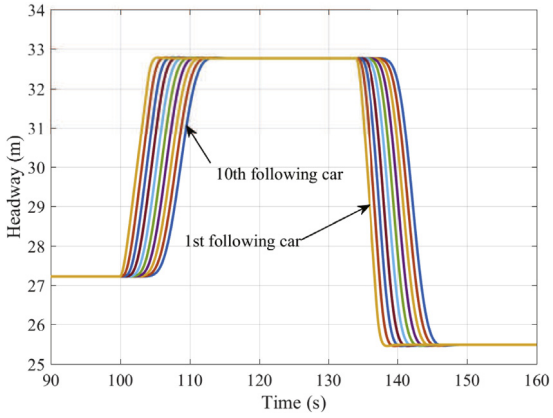
The used parameters in Eq. (29) are presented in Table 1, where $y_{\min}$ represents minimum headway which is a critical value to judge whether the traffic collision arises, i.e., if the current headway is smaller than $y_{\min}$, traffic collision turns unavoidable; T indicates a sampling time that selects data with a regular interval [58,101].



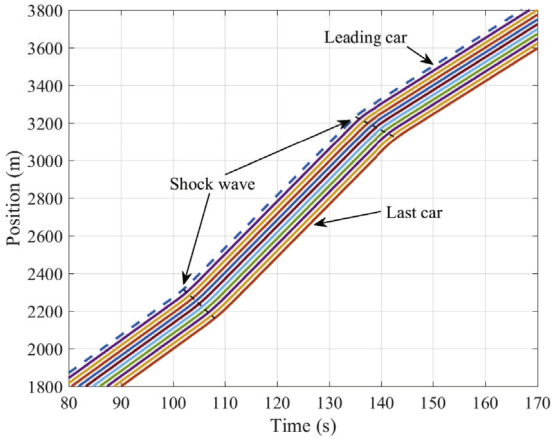
(a) Velocity–time patterns with no attack.



(b) Space–time patterns with no attack.



(c) Headway–time patterns with no attack.



(d) Position–time patterns with no attack.

Fig. 7. Time evolutions of the velocity and space profiles for base scenario.

Table 1
Simulation parameters of vehicles.

Parameter	Value	Unit	Description
η	25.0	m	Safety distance
ξ	23.3	m	Distance parameter
$v_{\max}$	33.6	m/s	Maximum velocity
v	20	m/s	Initial velocity
$y_{\min}$	7.02	m	Minimum headway
T	0.1	s	Sampling time

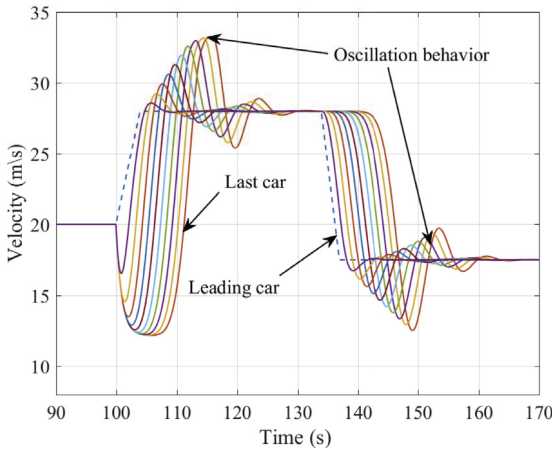
Now, we assume that a connected vehicle platoon consisted of 11 cars is moving on a single lane without lane-changing and overtaking behaviors, and vehicles are communicated using look-ahead-to-the-direct-leader topology (see Fig. 6). The initial conditions are set as follows:

$$\begin{cases} v_n(0) = 20 \text{ m/s}, \ n = 1, \ \ldots, 11; \\ x_1(0) = 0; \\ \Delta x_n(0) = v\xi/v_{\max} \ - \xi/2 \ + \eta = 27.22 \text{ m}, \ \ n = 1, \ \ldots, 10, \end{cases} \tag{30}$$

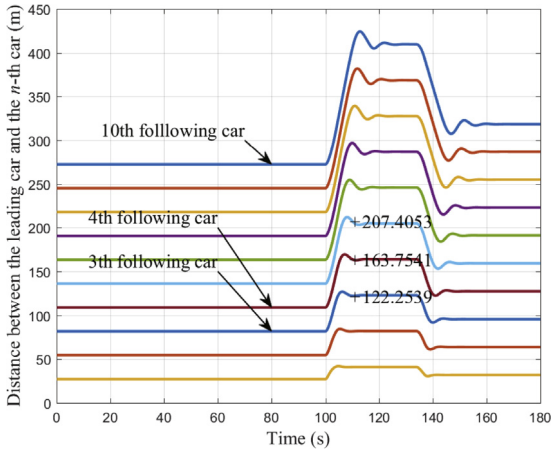
where $x_1(0)$ indicates the position of the last car (i.e., 11th car) at time $t = 0$, $v_1(0)$ indicates the velocity of the last car (i.e., 11th car) at time $t = 0$, $v_{11}(0)$ indicates the velocity of the first car (i.e., leading car) at time $t = 0$, $\Delta x_{10}(0)$ indicates the distance difference between the leading car and the first following car (i.e., 2th car in the platoon) at time $t = 0$.

Table 2
4 scenarios for experiment analysis.

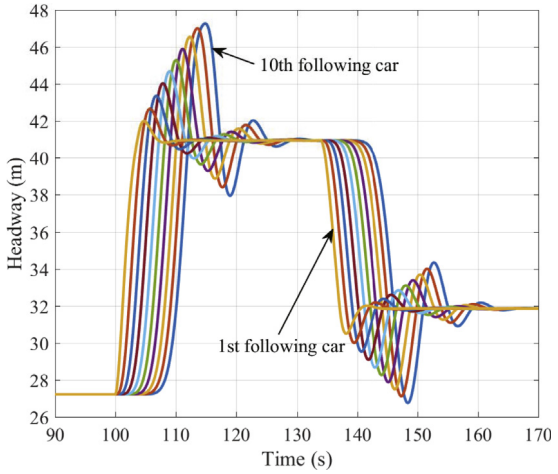
Scenario	Description	Altered parameter	Possible attacks
0	No attack; 10 vehicles are following the first leading vehicle with a uniform speed and headway at the beginning; traffic fluctuation occurs during 100–150s.	\	No attacks
1	Attacks interferes the communication between cars, forcing cars to downgrade to ACC mode or manual operations.	α	DoS
2	Attacks occur, leading the traveling platoon adopts unrealistic (i.e. underestimated or overestimated) headways or speeds.	Δv_n, Δx_n	*Falsification, Masquerading*
3	Attacks repeat the previous messages without any update of real-time information about distance difference and velocity difference from its preceding car.	$\frac{d^2 x_n(t)}{dt^2}$	*Replay, Suppression, Falsification, Masquerading*



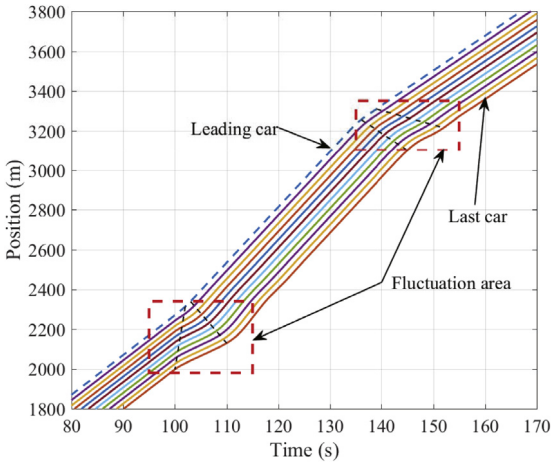
(a) Velocity–time patterns with communication failure.



(b) Space–time patterns with communication failure.



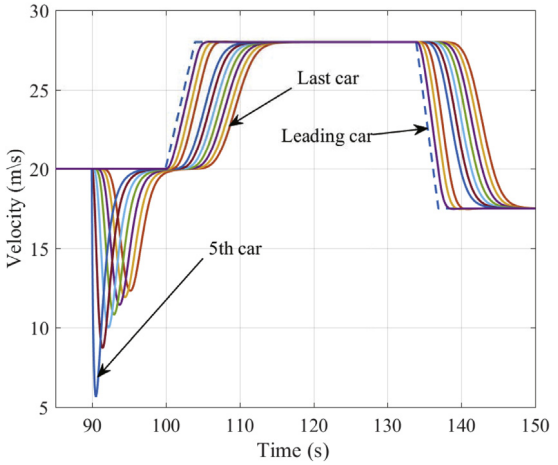
(c) Headway–time patterns with communication failure.



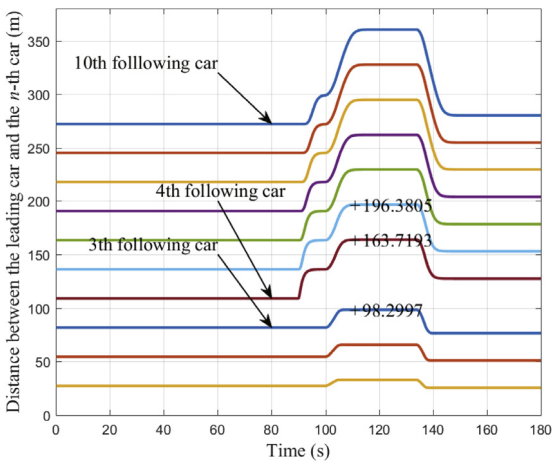
(d) Position–time patterns with communication failure.

Fig. 8. Time evolutions of the velocity and space profiles for Scenario 1.

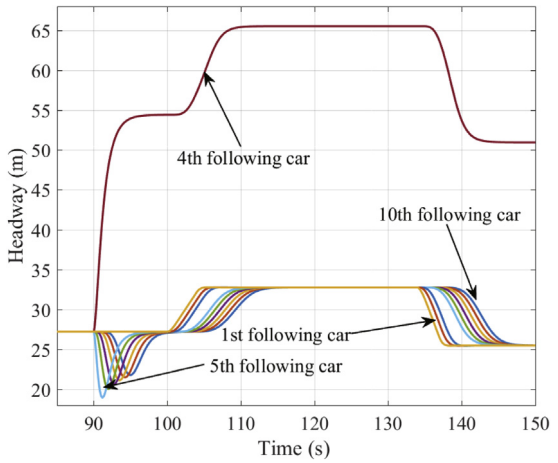
As mentioned above, all vehicles in the platoon are assumed to have identical velocity and headway at the early stage. But once the wireless communication is interfered by cyberattacks, traffic parameters including velocity, inter-vehicle distance, and acceleration may be drastically changed. To better demonstrate the impacts of attacks, we design the following 4 scenarios in later section. First, a summary of these 4 scenarios are presented in Table 2:



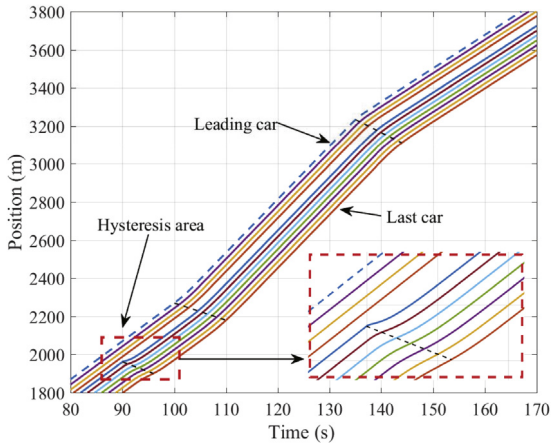
(a) Velocity–time patterns with underestimated headway.



(b) Space–time patterns with underestimated headway.



(c) Headway–time patterns with underestimated headway.



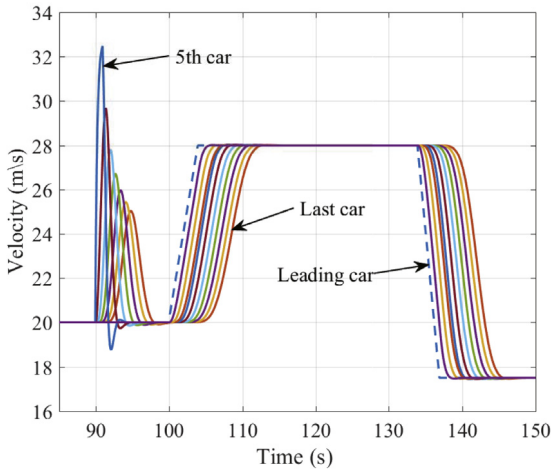
(d) Position–time patterns with underestimated headway.

Fig. 9. Time evolutions of the velocity and space profiles with underestimated headway.

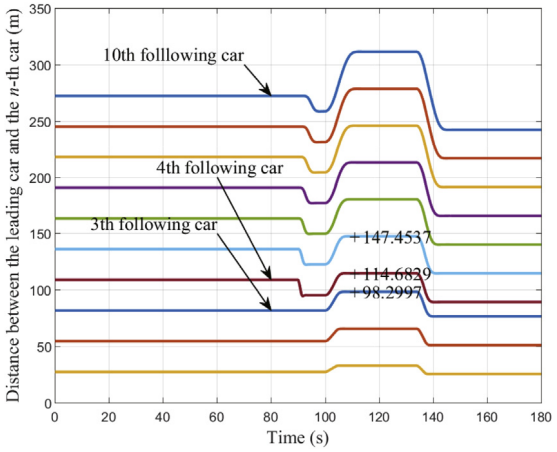
(1) Scenario 0: base scenario without cyberattacks

The base scenario is regarded as a reference to compare with other cases with cyberattacks. In Scenario 0, we assume that 10 vehicles are following the first leading vehicle with a uniform velocity of $v = 20$ m/s and headway of $h = 27.22$ m on a single lane with no attacks in the early time. The traffic flow is stable and it can fluctuate smoothly along with leading car's movement. Given that the wireless communication and sensors perceiving between each two connected vehicles, we set each vehicle controller's sensitivity as $\alpha = 3.0\ \mathrm{s}^{-1}$ that is slightly larger than the traditional driver's sensitivity [106–108]. To show the dynamics of traffic, we set some velocity changes to the first leading car. In detail, during $100 - 104$ s, the first leading car speeds up with an acceleration of $2\ \mathrm{m/s}^2$; and then retains a constant speed of $v = 28$ m/s during $105 - 133$ s. During $134 - 137$ s, the vehicle slows down with a deceleration of $3.5\ \mathrm{m/s}^2$; and then keeps a constant speed of $v = 17.5$ m/s during the remaining time. In this case, the speed dynamics for other following cars can be updated through our model Eq. (7) with $p = q = 1$, which is equivalent to the classical RV model without cyberattacks.

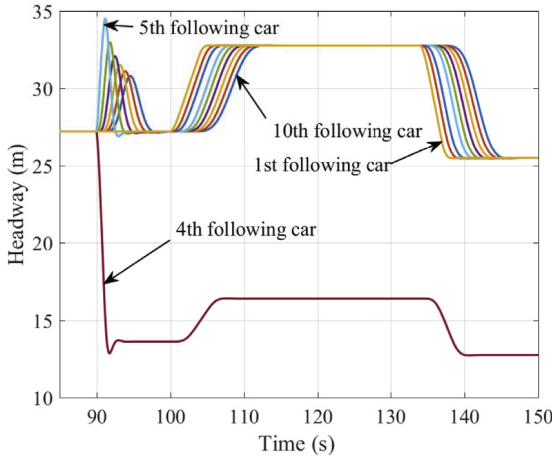
To describe the base scenario intuitively, Fig. 7 is plotted to show the velocity–time, space–time, headway–time and position–time patterns. Fig. 7a shows the velocity change of each car with time; Fig. 7b shows the change of the distance between each following car and the first leading car; Fig. 7c shows the change of each following car's headway; and Fig. 7d shows the position change of each vehicle. From the figure, a disturbance happens at $t = 100$ s and shockwave propagates backwards during $100 - 142$ s. These subfigures can clearly describe the evolution of velocity and space patterns with time for connected vehicles during no attacks. For future comparisons, at $t = 110$ s, the distance values of the 3rd following car and the leading car (i.e., 98.2997 m), the 4th following car and the leading car (i.e., 131.0684 m), and the 5th following car and the leading car (i.e., 163.846 m) are marked in Fig. 7b.



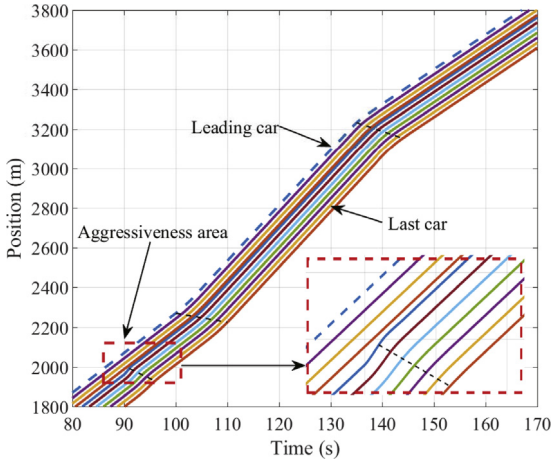
(a) Velocity–time patterns with overestimated headway.



(b) Space–time patterns with overestimated headway.



(c) Headway–time patterns with overestimated headway.



(d) Position–time patterns with overestimated headway.

Fig. 10. Time evolutions of the velocity and space profiles with overestimated headway.

(2) Scenario 1: Communication failure

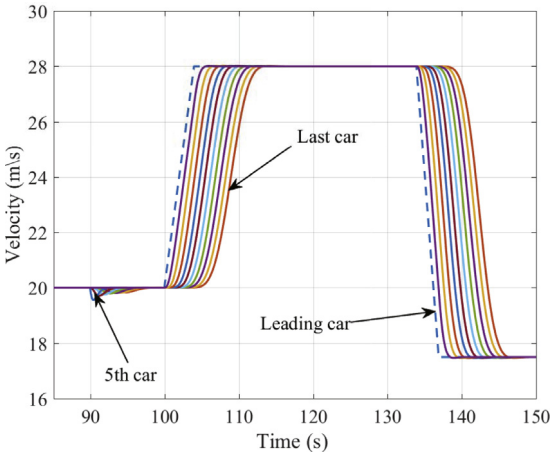
It is known that some attacks may interfere the communication between vehicles, then connected vehicles may lose the information from other vehicles. Such failure can force the connected vehicles to downgrade to ACC mode or even manual operations. To simulate such circumstance, the sensitivity α in Eq. (7) will be altered in light of the severity degree caused by cyberattacks. In our experiment, a communication failure occurs at $t = 100$ s, and the vehicles' sensitivity is altered to $\alpha = 1.0\ \mathrm{s}^{-1}$, which is a recommended value for manual operation [96,107].

Fig. 8 presents velocity and space patterns for connected vehicles with communication failure. It can be seen that altering α could result in dramatic fluctuation of traffic. This attack deactivates wireless communication and prevents the target car from handling the incoming message. In this case, vehicles may have to downgrade to the ACC mode or even to manually driving mode, thereby causing significant oscillations, traffic congestions and even potential collisions. We would like to point out that in real world, when communication failure happens, the traffic could become worse since switching from autonomous control to manual driving will require additional reaction time.

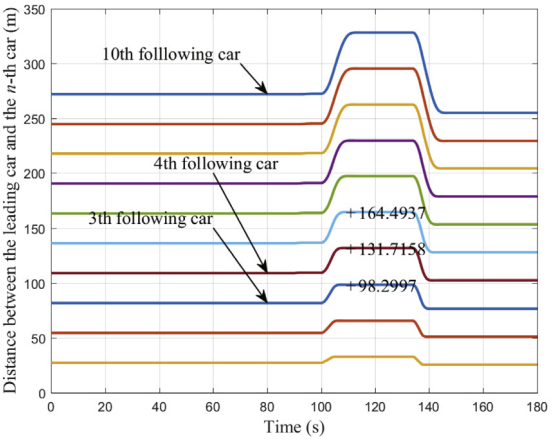
(3) Scenario 2: modification of headway/velocity

This case is set for the situations when attacks like *falsification* and *spoof* occur, leading the traveling platoon adopts unrealistic (i.e. underestimated or overestimated) headways or speeds. Without loss of generality, we list the following detailed cases:

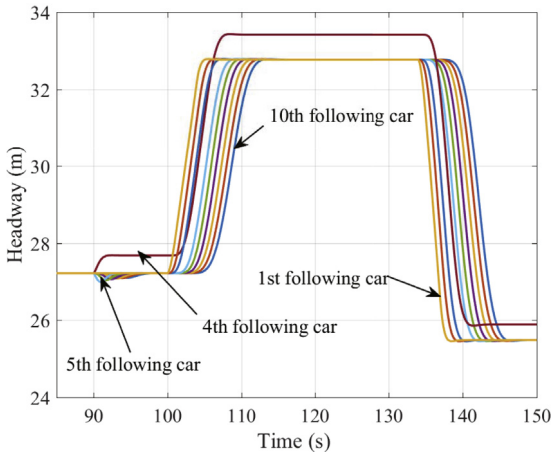
(1) Case I: The 5th car (i.e., $n = 7$) receives the 0.5 times (i.e., underestimated) of its real headway (see Fig. 9);
(2) Case II: The 5th car receives the 2 times (i.e., overestimated) of its real headway (see Fig. 10);



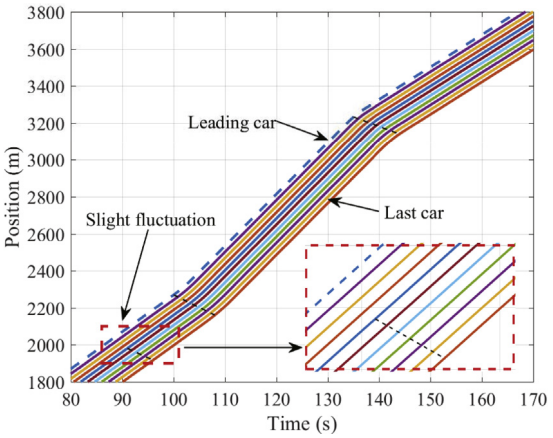
(a) Velocity–time patterns with underestimated velocity.



(b) Space–time patterns with underestimated velocity.



(c) Headway–time patterns with underestimated velocity.



(d) Position–time patterns with underestimated velocity.

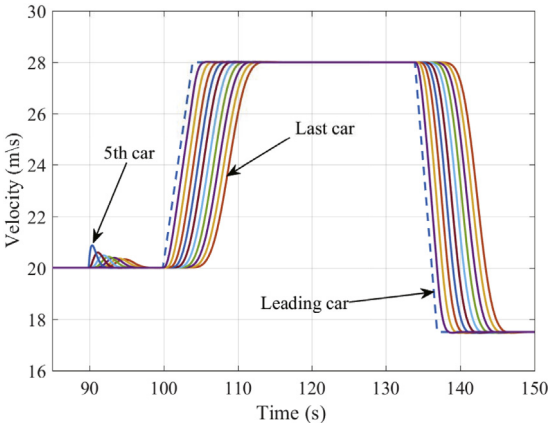
Fig. 11. Time evolutions of the velocity and space profiles with underestimated velocity message.

(3) Case III: The 5th car receives the 0.5 times (i.e., underestimated) of its preceding car's velocity (see Fig. 11);
(4) Case IV: The 5th car receives the 2 times (i.e., overestimated) of its preceding car's velocity (see Fig. 12).

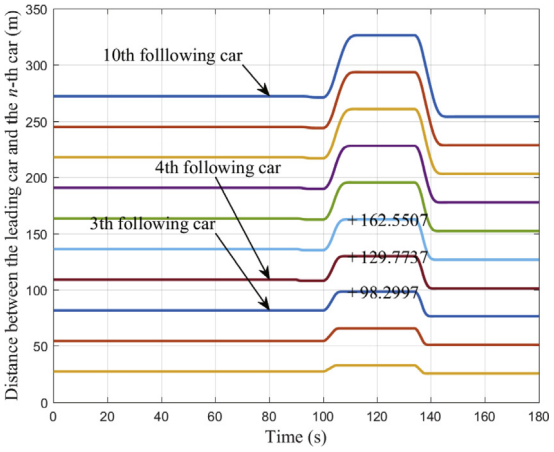
In scenario 2, attacks are assumed only happened to the 5th car. Particularly, Fig. 9 shows the velocity and space profiles with the 5th car receiving underestimated (0.5 time) headway; and Fig. 10 shows the velocity and space profiles with the 5th car receiving overestimated (2 time) headway. From these two figures, we can find that both overestimated and underestimated headways can cause traffic oscillation. By comparison, attacks with overestimated headway lead to bigger traffic oscillation, therefore, traffic becomes more unstable and less safe; while attacks with underestimated headway improve the stability of the traffic but causing longer headway and lower traffic volume. Moreover, these simulation results are in line with theoretical results, please refer to Fig. 2.

Similarly, Figs. 11 and 12 present the simulation results for the cases with underestimated and overestimated velocity, respectively. Fig. 11 presents the velocity and space patterns with the 5th car receiving underestimated (0.5 time) velocity, and Fig. 12 presents the velocity and space patterns with 5th car receiving overestimated (2 time) velocity. In the same way, we can find that attacks with overestimated velocity cause bigger traffic oscillations so traffic becomes more unstable and less safe, but attacks with underestimated velocity cause slightly traffic oscillation.

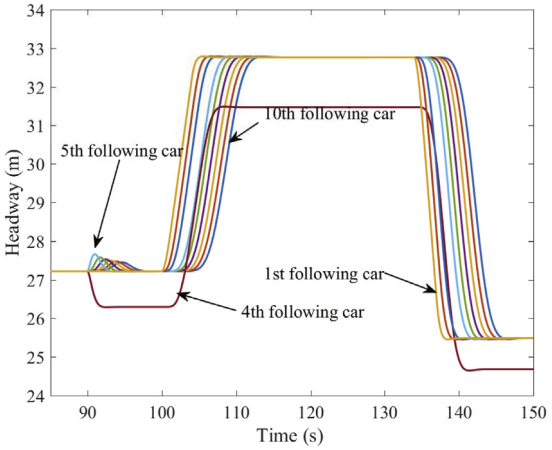
In addition, by comparing false headway information (Figs. 9 and 10) with false velocity information (Figs. 11 and 12), it can be seen that the fluctuation amplitudes for velocity and headway in Figs. 9 and 10 are significantly larger than that in Figs. 11 and 12. In other words, false headway information may bring more serious impacts to traffic than that caused by false velocity information. In fact, this observation is in accordance with theoretical results (see Figs. 3 and 4) and real situation, i.e., drivers pay more attention to the distance from the preceding car (i.e., safety gap) than the speed of the preceding car.



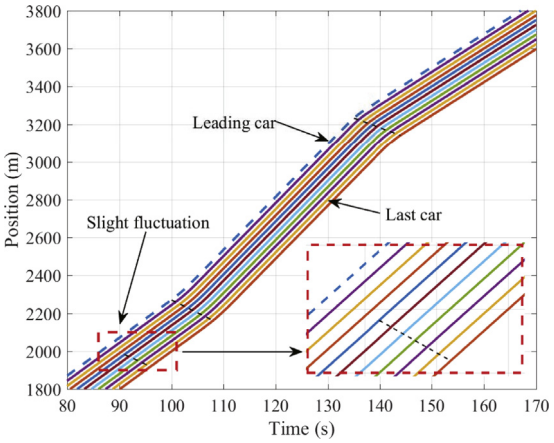
(a) Velocity–time patterns with overestimated velocity.



(b) Space–time patterns with overestimated velocity.



(c) Headway–time patterns with overestimated velocity.



(d) Position–time patterns with overestimated velocity.

Fig. 12. Time evolutions of the velocity and space profiles with overestimated velocity message.

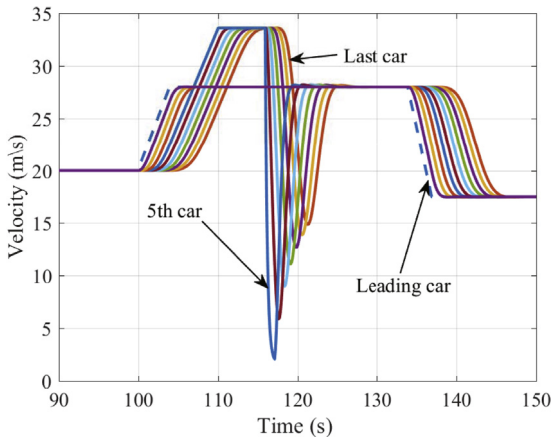
(4) Scenario 3: Alteration of acceleration/deceleration

Some attacks like relay and suppression can store and repeat the previous messages. To describe this circumstance, we assume that an attacked car keeps its old acceleration information with ignoring real-time information about headway and relative velocity from its preceding car. It is no doubt that such malicious behavior could cause potential rear-end accidents and significant traffic oscillation. Particularly, we simulate two cases:

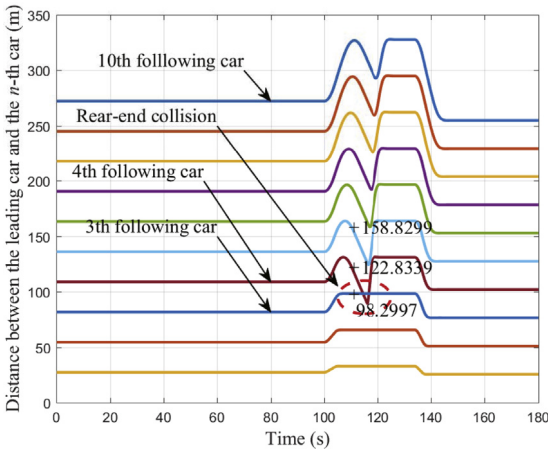
(1) Case I: An adversary stores the acceleration message of the 5th car at $t = 104$ s and send the stored message to the 5th car for the following 12 s;
(2) Case II: An adversary stores the deceleration message of the 5th car at $t = 137$ s and send the stored message to the 5th car for the following 20 s.

For Case I, as shown in Fig. 13, we present the evolution of velocity, space, headway, and position with replaying acceleration information. In Fig. 13a, the attacked car follows the wrong acceleration messages and keeps accelerating until the maximum speed (i.e., $v_{\max}$). When the attack ends, the attacked car recovers its "sense" and immediately slows down to avoid any accidents. However, in this test, a car crash has happened as shown in Figs. 13b–d. Notice that if many cars moving in road network are infected by this attack, no doubt, a massive of pile-up accidents or gridlock will arise.

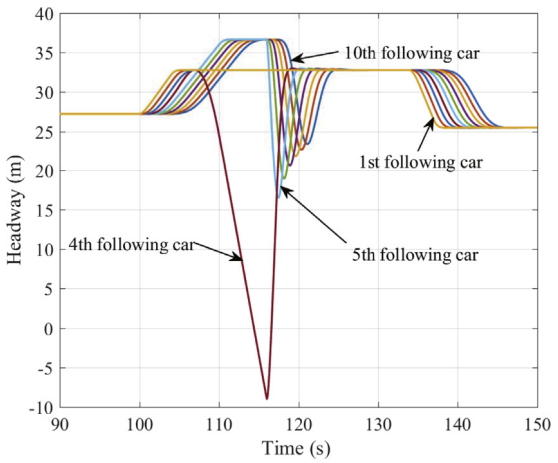
For Case II, we present velocity, space, headway, and position patterns with replaying deceleration information in Fig. 14. When the attack happens, the target car continuously decelerates for a period of attacking time. Hence, the gap between the attacked car and its preceding car has been significantly enlarged. Obviously, such attacks seriously decline traffic volume, and influence the efficiency of the whole system. Note that we have set each vehicle's velocity not less than zero to avoid any unreasonable situations like vehicle backing up on a road. Therefore, although it looks that the velocity of following vehicles



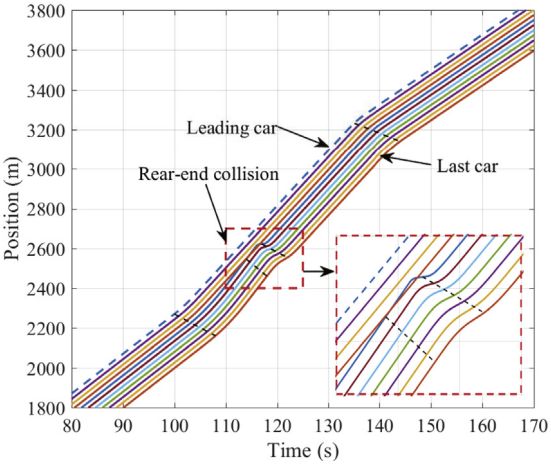
(a) Velocity–time plots with acceleration attack.



(b) Space–time patterns with acceleration attack.



(c) Headway–time patterns with acceleration attack.



(d) Position–time patterns with acceleration attack.

Fig. 13. Time evolutions of the velocity and space profiles with acceleration attacks.

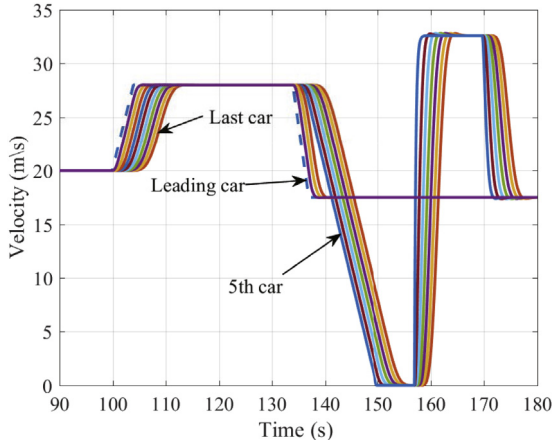
in Fig. 14(a) will become negative during the time gap 150s–160 s following the trend, the vehicle actually will reach a complete stop after deceleration. Therefore, the velocity of following vehicles in Fig. 14(a) will not be negative during the following time gap, but become zero.

As discussed above, four scenarios are performed and we know that cyberattacks may cause traffic disturbance, potential congestion and even rear-end collision. To further discuss the traffic impacts, we provide the following table to investigate the travel delay time under different experiment scenarios. In Table 3, the first column indicates the position of the last car, the other columns indicate the travel time when the last car passing by some given positions under different scenarios.

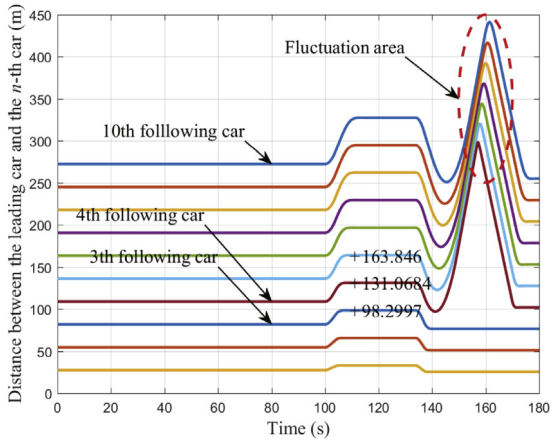
As shown in Table 3, the travel time of the connected vehicles is impacted by cyberattacks. Comparing scenarios 1–3 with base scenario 0, we can see that some malicious behavior in scenario 1, case II of scenario 2 and case II of scenario 3 can bring out significantly travel delay. However, some attacks may decrease travel time but at the price of shrinking safety gap. No doubt, such radical behaviors could cause a potential jams and rear-end collisions.

6. Concluding remarks

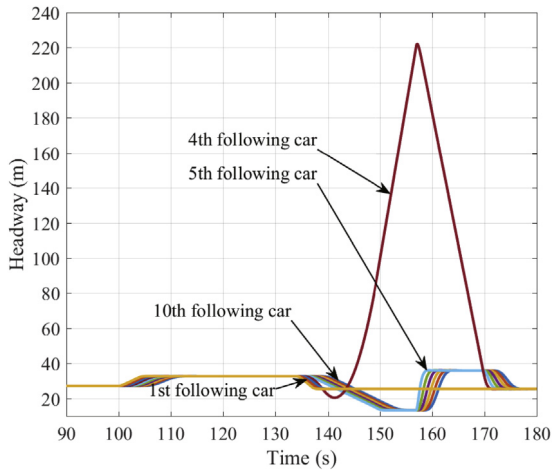
With the advent of connected vehicles technology, cybersecurity on vehicles has drew many scholars' attention. This model is extended from a classical car-following model by adding two weight coefficients which are able to quantify the impacts from cyberattacks. Then applying the linear stability theory and reductive perturbation method, we carry out the linear and nonlinear stability analysis and obtain the stable, metastable and unstable regions. Finally, using simulation, our model is further evaluated and verified. Numerical results demonstrate that the dynamic change of connected vehicles is indeed impacted by security threats as well as different cyberattacks are able to lead to different traffic fluctuation patterns



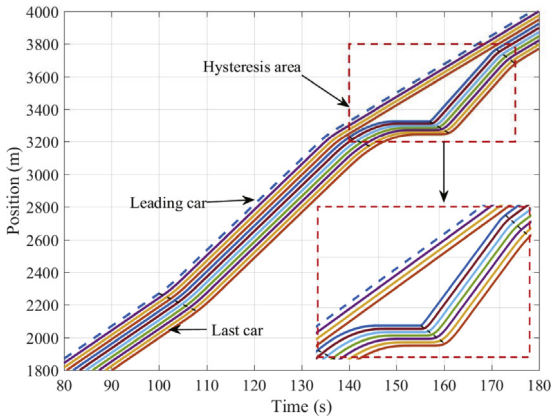
(a) Velocity–time plots with deceleration attack.



(b) Space–time patterns with deceleration attack.



(c) Headway–time patterns with deceleration attack.



(d) Position–time patterns with deceleration attack.

Fig. 14. Time evolutions of the velocity and space profiles with deceleration attacks.

Table 3
Travel time of the last car at given positions with different scenarios.

$x_1(m)$	Scenario 0(s)	Scenario 1(s)	Scenario 2(s)				Scenario 3(s)	
			Case I	Case II	Case III	Case IV	Case I	Case II
1800	90.1	90.1	90.1	90.1	90.1	90.1	90.1	90.1
2000	100.1	100.1	101.5	99.4	100.1	100.1	100.1	100.1
2200	109.7	113.2	110.8	109.1	109.7	109.6	109.7	109.7
2400	116.9	119.8	118.1	116.3	116.9	116.8	116.2	116.9
2600	124.0	126.9	125.2	123.4	124.1	124.0	124.0	124.1
2800	131.2	134.1	132.4	130.6	131.2	131.1	131.2	131.2
3000	138.3	141.3	139.5	137.7	138.3	138.3	138.3	138.3
3200	147.3	151.2	148.8	146.6	147.4	147.2	147.3	147.3
3400	158.7	162.4	160.2	158.0	158.8	158.7	158.7	166.1
3600	170.2	173.8	171.6	169.4	170.2	170.1	170.2	172.3

including traffic jams, delay and rear-end collisions. Our study aims to describe the effect of malicious attacks on connected vehicles. In some ways, the proposed model can bring inspiration to address other similar issue such aerial navigation and driverless trains in the context of cybersecurity.

Note our main focus of this paper is to model traffic dynamics with the potential cyberattacks. Therefore, we do not consider the physical limits of engine power and brake capability, and assume that commanded acceleration/deceleration can be achieved instantaneously without a time lag. Further exploration of the impacts of these physical limits will be

conducted in our future work. In addition, it is expected this research could also help counter the detrimental effects caused by cyberattacks. By understanding the impacts on traffic dynamics caused by different types of cyberattacks, corresponding traffic control and management strategies could be developed and applied to resolve these impacts. The details of these strategies will be left for future research.

Acknowledgments

This research was supported by the National Key Research and Development Program of China (No. 2016YFB0100902).

References

[1] W. Liao, A. Tordeux, A. Seyfried, M. Chraibi, K. Drzycimski, X. Zheng, Y. Zhao, Measuring the steady state of pedestrian flow in bottleneck experiments, Physica A 461 (2016) 248–261.
[2] R.C. Carlson, I. Papamichail, M. Papageorgiou, A. Messmer, Optimal mainstream traffic flow control of large-scale motorway networks, Transp. Res. C 18 (2010) 193–212.
[3] G. Zhang, M. Zhao, D. Sun, W. Liu, H. Li, Stabilization effect of multiple drivers desired velocities in car-following theory, Physica A 442 (2016) 532–540.
[4] M.A.S. Kamal, J. Imura, T. Hayakawa, A. Ohata, K. Aihara, Smart driving of a vehicle using model predictive control for improving traffic flow, IEEE Trans. Intell. Transp. Syst. 15 (2014) 878–888.
[5] Y. Li, B. Yang, T. Zheng, Y. Li, M. Cui, S. Peeta, Extended-state-observer-based double-loop integral sliding-mode control of electronic throttle valve, IEEE Trans. Intell. Trans. Syst. 16 (2015) 2501–2510.
[6] E.B. Hamida, H. Noura, W. Znaidi, Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures, Electronics 4 (2015) 380–423.
[7] M.N. Mejri, M. Hamdi, Recent advances in cryptographic solutions for vehicular networks, in: 2015 International Symposium on Networks, Computers and Communications, ISNCC, IEEE, pp. 1–7.
[8] F. Qu, Z. Wu, F.Y. Wang, W. Cho, A security and privacy review of VANETs, IEEE Trans. Intell. Transp. Syst. 16 (2015) 2985–2996.
[9] S. Woo, H.J. Jo, D.H. Lee, A practical wireless attack on the connected car and security protocol for in-vehicle CAN, IEEE Trans. Intell. Transp. Syst. 16 (2015) 993–1006.
[10] R.G. Engoulou, M. Bellaïche, S. Pierre, A. Quintero, VANET security surveys, Comput. Commun. 44 (2014) 1–13.
[11] J. Reilly, S. Martin, M. Payer, A.M. Bayen, Creating complex congestion patterns via multi-objective optimal freeway traffic control with application to cyber-security, Transp. Res. B 91 (2016) 366–382.
[12] M. Amoozadeh, A. Raghuramu, C. Chuah, D. Ghosal, H.M. Zhang, J. Rowe, K. Levitt, Security vulnerabilities of connected vehicle streams and their impact on cooperative driving, IEEE Commun. Mag. 53 (2015) 126–132.
[13] S. Dadras, R.M. Gerdes, R. Sharma, Vehicular platooning in an adversarial environment, in: The 10th ACM Symposium on Information, Computer and Communications Security, ACM, pp. 167–178.
[14] R.M. Gerdes, C. Winstead, K. Heaslip, CPS: An efficiency-motivated attack against autonomous vehicular transportation, in: The 29th Annual Computer Security Applications Conference, ACM, pp. 99–108.
[15] D.C. Gazis, The origins of traffic theory, Oper. Res. 50 (2002) 69–77.
[16] H. Greenberg, An analysis of traffic flow, Oper. Res. 7 (1959) 79–85.
[17] D. Ngoduy, Platoon-based macroscopic model for intelligent traffic flow, Transportmetrica B: Trans. Dyn. 1 (2013) 153–169.
[18] Y. Li, D. Sun, W. Liu, M. Zhang, M. Zhao, X. Liao, L. Tang, Modeling and simulation for microscopic traffic flow based on multiple headway, velocity and acceleration difference, Nonlinear Dynam. 66 (2011) 15–28.
[19] Y. Li, L. Zhang, S. Peeta, H. Pan, T. Zheng, Y. Li, X. He, Non-lane-discipline-based car-following model considering the effects of two-sided lateral gaps, Nonlinear Dynam. 80 (2015) 227–238.
[20] A. Reuschel, Vehicle movements in a platoon with uniform acceleration or deceleration of the lead vehicle, Zeitschrift Des Oesterreichischen Ingenieur-Und Architekten-Vereines 95 (1950) 50–62.
[21] L.A. Pipes, An operational analysis of traffic dynamics, J. Appl. Phys. 24 (1953) 274–281.
[22] R.E. Chandler, R. Herman, E.W. Montroll, Traffic dynamics: Studies in car following, Oper. Res. 6 (1958) 165–184.
[23] G.F. Newell, Nonlinear effects in the dynamics of car following, Oper. Res. 9 (1961) 209–229.
[24] E. Kometani, T. Sasaki, A safety index for traffic with linear spacing, Oper. Res. 7 (1959) 704–720.
[25] E. Kometani, T. Sasaki, Dynamic behaviour of traffic with a non-linear spacing-speed relationship, in: Proceedings of Transportation Research Board, pp. 105–119.
[26] P.G. Gipps, A behavioural car-following model for computer simulation, Transp. Res. B 15 (1981) 105–111.
[27] R. Benekohal, J. Treiterer, Carsim: Car-following model for simulation of traffic in normal and stop-and-go conditions, Transp. Res. Rec. (1988) 99–111.
[28] W. Helly, Simulation of bottlenecks in single-lane traffic flow, in: Proceedings of the Symposium on Theory of Traffic Flow, General Motors Research Laboratories, New York, pp. 207–238.
[29] A. Hanken, T. Rockwell, A model of car-following derived empirically by price-wise regression analysis in vehicular traffic science, in: Proceedings of the Third International Symposium on the Theory of Traffic Flow, Transportation Research Board, New York.
[30] J. Xing, A parameter identification of a car-following model, in: Steps Forward. Intelligent Transport Systems World Congress, Transportation Research Board, Yokohama, Japan, p. 1741.
[31] J. Vasic, H.J. Ruskin, Cellular automata simulation of traffic including cars and bicycles, Physica A 391 (2012) 2720–2729.
[32] T.J. Duff, D.M. Chong, K.G. Tolhurst, Using discrete event simulation cellular automata models to determine multi-mode travel times and routes of terrestrial suppression resources to wildland fires, European J. Oper. Res. 241 (2015) 763–770.
[33] R. Barlovic, L. Santen, A. Schadschneider, M. Schreckenberg, Metastable states in cellular automata for traffic flow, Eur. Phys. J. B 5 (1998) 793–800.
[34] R. Michaels, Perceptual factors in car following, in: Proceedings of the 2nd International Symposium on the Theory of Road Traffic Flow, OECD, Pair, pp. 44–59.
[35] J.J. Lee, J. Jones, Traffic dynamics: Visual angle car following models, Traffic Eng. Control 8 (1967) 348–350.
[36] K.L. Broughton, F. Switzer, D. Scott, Car following decisions under three visibility conditions and two speeds tested with a driving simulator, Accid. Anal. Prevent. 39 (2007) 106–116.
[37] P. Chakroborty, S. Kikuchi, Calibrating the membership functions of the fuzzy inference system: Instantiated by car-following data, Transp. Res. C 11 (2003) 91–119.
[38] S. Kikuchi, P. Chakroborty, Car-following model based on fuzzy inference system, Transp. Res. Rec. (1992) 82–82.
[39] H. Hao, W. Ma, H. Xu, A fuzzy logic-based multi-agent car-following model, Transp. Res. C 69 (2016) 477–496.

[40] M. McDonald, J. Wu, M. Brackstone, Development of a fuzzy logic based microscopic motorway simulation model, in: IEEE Conference on Intelligent Transportation System, IEEE, pp. 82–87.
[41] Y. Li, L. Zhang, H. Zheng, X. He, S. Peeta, T. Zheng, Y. Li, Nonlane-discipline-based car-following model for electric vehicles in transportation-cyber-physical systems, IEEE Trans. Intell. Transp. Syst. (2017). http://dx.doi.org/10.1109/TITS.2017.2691472.
[42] M. Bando, K. Hasebe, A. Nakayama, A. Shibata, Y. Sugiyama, Dynamical model of traffic congestion and numerical simulation, Phys. Rev. E 51 (1995) 1035–1042.
[43] J. Zhao, P. Li, An extended car-following model with consideration of speed guidance at intersections, Physica A 461 (2016) 1–8.
[44] T. Nagatani, K. Nakanishi, H. Emmerich, Phase transition in a difference equation model of traffic flow, J. Phys. A: Math. Gen. 31 (1998) 5431–5438.
[45] H. Ge, S. Dai, Y. Xue, L. Dong, Stabilization analysis and modified Korteweg–de Vries equation in a cooperative driving system, Phys. Rev. E 71 (2005) 1–7.
[46] Y. Li, L. Zhang, B. Zhang, T. Zheng, H. Feng, Y. Li, Non-lane-discipline-based car-following model considering the effect of visual angle, Nonlinear Dynam. 85 (2016) 1901–1912.
[47] K. Aghabayk, M. Sarvi, W. Young, A state-of-the-art review of car-following models with particular considerations of heavy vehicles, Transp. Rev. 35 (2015) 82–105.
[48] Z. Li, L. Liu, S. Xu, Y. Qian, Impact of driving aggressiveness on the traffic stability based on an extended optimal velocity model, Nonlinear Dynam. 81 (2015) 2059–2070.
[49] T.Q. Tang, L. Chen, H.J. Huang, Z.Q. Song, Analysis of the equilibrium trip cost without late arrival and the corresponding traffic properties using a car-following model, Physica A 460 (2016) 348–360.
[50] S. Yu, X. Zhao, Z. Xu, L. Zhang, The effects of velocity difference changes with memory on the dynamics characteristics and fuel economy of traffic flow, Physica A 461 (2016) 613–628.
[51] J. Monteil, R. Billot, J. Sau, N.E.E. Faouzi, Linear and weakly nonlinear stability analyses of cooperative car-following models, IEEE Trans. Intell. Transp. Syst. 15 (2014) 2001–2013.
[52] S. Yu, Z. Shi, An improved car-following model considering relative velocity fluctuation, Commun. Nonlinear Sci. Numer. Simul. 36 (2016) 319–326.
[53] A. Kesting, M. Treiber, D. Helbing, Enhanced intelligent driver model to access the impact of driving strategies on traffic capacity, Philos. Trans. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci. 368 (2010) 4585–4605.
[54] G. Peng, W. Lu, H. He, Z. Gu, Nonlinear analysis of a new car-following model accounting for the optimal velocity changes with memory, Commun. Nonlinear Sci. Numer. Simul. 40 (2016) 197–205.
[55] D. Ngoduy, R. Wilson, Multianticipative nonlocal macroscopic traffic model, Comput.-Aided Civil Infrastruct. Eng. 29 (2014) 248–263.
[56] Y. Li, L. Zhang, S. Peeta, X. He, T. Zheng, Y. Li, A car-following model considering the effect of electronic throttle opening angle under connected environment, Nonlinear Dynam. 85 (2016) 2115–2125.
[57] T. Tang, W. Shi, H. Shang, Y. Wang, A new car-following model with consideration of inter-vehicle communication, Nonlinear Dynam. 76 (2014) 2017–2023.
[58] G. Yu, P. Wang, X. Wu, Y. Wang, Linear and nonlinear stability analysis of a car-following model considering velocity difference of two adjacent lanes, Nonlinear Dynam. 84 (2016) 387–397.
[59] Y. Jin, M. Xu, Stability analysis in a car-following model with reaction-time delay and delayed feedback control, Physica A 459 (2016) 107–116.
[60] M. Muramatsu, T. Nagatani, Soliton and kink jams in traffic flow with open boundaries, Phys. Rev. E 60 (1999) 180–187.
[61] X. Yu, Analysis of the stability and density waves for traffic flow, Chin. Phys. 11 (2002) 1128.
[62] K. Hasebe, A. Nakayama, Y. Sugiyama, Equivalence of linear response among extended optimal velocity models, Phys. Rev. E 69 (2004) 1–3.
[63] K. Hasebe, A. Nakayama, Y. Sugiyama, Dynamical model of a cooperative driving system for freeway traffic, Phys. Rev. E 68 (2003) 1–6.
[64] J. Zhou, Z. Shi, J. Cao, Nonlinear analysis of the optimal velocity difference model with reaction-time delay, Physica A 396 (2014) 77–87.
[65] J. Petit, S.E. Shladover, Potential cyberattacks on automated vehicles, IEEE Trans. Intell. Transp. Syst. 16 (2015) 546–556.
[66] W. Li, H. Song, Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 17 (2016) 960–969.
[67] I. Sajjad, D.D. Dunn, R. Sharma, R. Gerdes, Attack mitigation in adversarial platooning using detection-based sliding mode control, in: Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, ACM, pp. 43–53.
[68] M. Amoozadeh, H. Deng, C.-N. Chuah, H.M. Zhang, D. Ghosal, Platoon management with cooperative adaptive cruise control enabled by VANET, Veh. Commun. 2 (2015) 110–123.
[69] J. Ploeg, E. Semsar-Kazerooni, G. Lijster, N. van de Wouw, H. Nijmeijer, Graceful degradation of CACC performance subject to unreliable wireless communication, in: 16th International IEEE Conference on Intelligent Transportation Systems, ITSC 2013, Hague, Netherlands, pp. 1210–1216.
[70] D. Chowdhury, L. Santen, A. Schadschneider, Statistical physics of vehicular traffic and some related systems, Phys. Rep. 329 (2000) 199–329.
[71] S. Yu, X. Zhao, Z. Xu, Z. Shi, An improved car-following model considering the immediately ahead car's velocity difference, Physica A 461 (2016) 446–455.
[72] Y. Jin, M. Xu, Stability analysis in a car-following model with reaction-time delay and delayed feedback control, Physica A 459 (2016) 107–116.
[73] T.Q. Tang, K.W. Xu, S.C. Yang, H.Y. Shang, Influences of battery exchange on the vehicles driving behavior and running time under car-following model, Measurement 59 (2015) 30–37.
[74] S. Yu, Z. Shi, Dynamics of connected cruise control systems considering velocity changes with memory feedback, Measurement 64 (2015) 34–48.
[75] L.J. Zheng, C. Tian, D.-H. Sun, W.N. Liu, A new car-following model with consideration of anticipation driving behavior, Nonlinear Dynam. 70 (2012) 1205–1211.
[76] L. Davis, Stability of adaptive cruise control systems taking account of vehicle response time and delay, Phys. Lett. A 376 (2012) 2658–2662.
[77] G. Whitham, Exact solutions for a discrete system arising in traffic flow, in: Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, vol. 428, The Royal Society, pp. 49–69.
[78] T. Nagatani, Stabilization and enhancement of traffic flow by the next-nearest-neighbor interaction, Phys. Rev. E 60 (1999) 6395–6401.
[79] Z.P. Li, Y.C. Liu, Analysis of stability and density waves of traffic flow model in an ITS environment, Eur. Phys. J. B 53 (2006) 367–374.
[80] S. Yu, Z. Shi, An extended car-following model considering vehicular gap fluctuation, Measurement 70 (2015) 137–147.
[81] T.Q. Tang, H.J. Huang, Z.Y. Gao, Stability of the car-following model on two lanes, Phys. Rev. E (3) 72 (2005) 1–7.
[82] T. Nagatani, Thermodynamic theory for the jamming transition in traffic flow, Phy. Rev. E 58 (1998) 4271–4276.
[83] R. Jiang, Q. Wu, Z. Zhu, Full velocity difference model for a car-following theory, Phy. Rev. E 64 (2001) 1–4.
[84] T. Nagatani, TDGL and MKdV equations for jamming transition in the lattice models of traffic, Physica A 264 (1999) 581–592.
[85] B.S. Kerner, P. Konhäuser, Cluster effect in initially homogeneous traffic flow, Phys. Rev. E 48 (1993) R2335–R2338.
[86] D. Ngoduy, Generalized macroscopic traffic model with time delay, Nonlinear Dynam. 77 (2014) 289–296.
[87] A. Nakayama, Y. Sugiyama, K. Hasebe, Effect of looking at the car that follows in an optimal velocity model of traffic flow, Phys. Rev. E 65 (2001) 016112.
[88] Y. Li, H. Zhu, M. Cen, Y. Li, R. Li, D. Sun, On the stability analysis of microscopic traffic car-following model: A case study, Nonlinear Dynam. 74 (2013) 335–343.

[89] R.E. Wilson, J.A. Ward, Car-following models: Fifty years of linear stability analysis–a mathematical perspective, Transp. Plan. Technol. 34 (2011) 3–18.
[90] R.E. Wilson, Mechanisms for spatio-temporal pattern formation in highway traffic models, Philos. Trans. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci. 366 (2008) 2017–2032.
[91] F. Liu, R. Cheng, P. Zheng, H. Ge, TDGL and MKdV equations for car-following model considering traffic jerk, Nonlinear Dynam. 83 (2016) 793–800.
[92] D.A. Kurtze, D.C. Hong, Traffic. jams, granular. flow, soliton. selection, Traffic jams granular flow soliton selection, Phys. Rev. E 52 (1995) 218–221.
[93] E. Tomer, L. Safonov, S. Havlin, Presence of many stable nonhomogeneous states in an inertial car-following model, Phys. Rev. Lett. 84 (2000) 382–385.
[94] P. Berg, A. Mason, A. Woods, Continuum approach to car-following models, Phys. Rev. E 61 (2000) 1056–1066.
[95] H.K. Lee, H.W. Lee, D. Kim, Macroscopic traffic models from microscopic car-following models, Phys. Rev. E 64 (2001) 1–12.
[96] H. Kuang, Z.P. Xu, X.L. Li, S.M. Lo, An extended car-following model accounting for the honk effect and numerical tests, Nonlinear Dynam. 87 (2017) 149–157.
[97] M.C. Cross, P.C. Hohenberg, Pattern formation outside of equilibrium, Rev. Modern Phys. 65 (1993) 851–1112.
[98] H. Ge, R. Cheng, S. Dai, KdV and kink–antikink solitons in car-following models, Physica A 357 (2005) 466–476.
[99] A.H. Nayfeh, Introduction to Perturbation Techniques, John Wiley & Sons, 2011.
[100] H.X. Ge, S.Q. Dai, L.Y. Dong, Y. Xue, Stabilization effect of traffic flow in an extended car-following model based on an intelligent transportation system application, Phys. Rev. E 70 (2004) 1–6.
[101] K. Konishi, H. Kokame, K. Hirata, Coupled map car-following model and its delayed-feedback control, Phys. Rev. E 60 (1999) 4000–4007.
[102] G. Hon.Xia, Modified coupled map car-following model and its delayed feedback control scheme, Chin. Phys. B 20 (2011) 1–8.
[103] M. Bando, K. Hasebe, K. Nakanishi, A. Nakayama, Analysis of optimal velocity model with explicit delay, Phys. Rev. E 58 (1998) 5429–5450.
[104] M. Bando, K. Hasebe, K. Nakanishi, A. Nakayama, A. Shibata, Y. Sugiyama, Phenomenological study of dynamical model of traffic flow, J. Physique I 5 (1995) 1389–1399.
[105] S.-i. Tadaki, M. Kikuchi, Y. Sugiyama, S. Yukawa, Coupled map traffic flow simulator based on optimal velocity functions, J. Phys. Soc. Japan 67 (1998) 2270–2276.
[106] T. Nagatani, Traffic jams induced by fluctuation of a leading car, Phys. Rev. E 61 (2000) 3534–3540.
[107] T. Nagatani, Jamming transition in a two-dimensional traffic flow model, Phys. Rev. E 59 (1999) 4857–4864.
[108] R. Wilson, P. Berg, S. Hooper, G. Lunt, Many-neighbour interaction and non-locality in traffic models, Eur. Phys. J. B 39 (2004) 397–408.