IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 10, 2020, accepted May 1, 2020, date of publication May 8, 2020, date of current version May 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2993254

Impact Evaluation of Cyber-Attacks on Traffic Flow of Connected and Automated Vehicles

CHANGYIN DONG[1,2,3], HAO WANG[1,2,3], DAIHENG NI[4], YONGFEI LIU[1,2,3], AND QUAN CHEN[1,2,3]

[1]School of Transportation, Southeast University, Nanjing 211189, China
[2]Jiangsu Key Laboratory of Urban ITS, Southeast University, Nanjing 211189, China
[3]Jiangsu Province Collaborative Innovation Center of Modern Urban Traffic Technologies, Southeast University, Nanjing 211189, China
[4]Department of Civil and Environmental Engineering, University of Massachusetts Amherst, Amherst, MA 01003, USA

Corresponding author: Hao Wang (haowang@seu.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFB1600900, in part by the National Natural Science Foundation of China under Grant 51878161 and Grant 71901223, and in part by the Postgraduate Research and Practice Innovation Program of Jiangsu Province under Grant KYCX17_0140.

ABSTRACT Connected and automated vehicles (CAVs) can improve transportation safety and efficiency based on vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communications. However, there are potential cyber threats to the communication systems via on-board unit equipped in CAVs and road-side unit. Based on existing traffic flow models, we design an evaluation framework for cyber-attacks on CAVs, and further investigate the impact of proportion of cyber-attacked vehicles, cyber-attack severity, cyber-attack range and traffic demand. Moreover, performance of the transportation system is analysed based on four indicators, including efficiency, safety, emissions and fuel consumption. The numerical simulation results show that with the increase of cyber-attacked vehicles and higher cyber-attack severity, the negative impact on traffic flow gradually becomes notable with lower capacity, higher risk of rear-end collision, more air pollutants and fuel consumption. In addition, it may lead to accidents and inefficient traffic operations if cyber-attacks occur on position rather than speed, and thus the position-attacked traffic system consumes more energy and emits more pollutants. The findings of this study provide useful information for the prediction of future cyber-attacked traffic, comprehensive evaluation of transportation systems, as well as management of automated highway systems from the perspective of network security.

INDEX TERMS Cyber-attack, cooperative adaptive cruise control, connected and automated vehicles, safety level.

I. INTRODUCTION

In recent years, connected and automated vehicles (CAVs) has been one of prospective applications within the field of intelligent transportation systems (ITS) in the future [1]–[3]. To predict potential emergencies about CAVs, simulation experiments designed for different traffic scenarios are a fundamental step before launching mature products into the market. To date, many car-following models have been proposed to describe characteristics of traffic flow from microscopic perspective [4]–[8]. The adaptive cruise control (ACC) system is one of the most popular applications designed for the control of longitudinal behaviors [9]–[12]. In addition, as an enhanced version of ACC, the cooperative adaptive cruise control (CACC) system can notably smooth hazardous traffic flow and improve traffic efficiency [4], [11], [13]–[19]. Li *et al.* developed an infrastructure-to-vehicle integrated system that incorporated both ACC and variable speed limit (VSL) to reduce rear-end collision risks on freeways [20]. Shladover *et al.* analyzed the advantages of CACC based on vehicle-to-vehicle (V2V) communication, including higher accuracy, faster response, and shorter gaps, resulting in enhanced traffic flow stability and possibly improved safety [17], [18], [21], [22]. In field test, several projects have been conducted for the system designs as well as empirical data analysis [18], [21], [23]. For example, the California Program on Advanced Technology for the Highway (PATH) attempted to design longitudinal controllers, providing an ideal basis for the following studies [11], [13], [14], [21], [24]–[28].

The associate editor coordinating the review of this manuscript and approving it for publication was Yue Cao.

However, advanced technologies always bring both opportunities and challenges. In the transportation field, the opportunities mean improvement of travel efficiency and traffic safety, while the challenges represent risk of cyber-attack, cost increase and moral issues when crashes happen [29]–[33]. In this paper, we focus on the cyber-attack via communications between on-board units and road-side units. In the previous theoretical researches, simulations have been extensively conducted to demonstrate the safety and stability of the cyber-attacked system [3], [12], [14], [31]–[41]. Particularly, Li *et al.* evaluated the influence of slight cyber-attacks on longitudinal safety of CAVs based on nine-vehicle experiments [14]. Wang *et al.* proposed an extended car-following model and analyzed the linear and nonlinear stability of the traffic flow under cyber-attack [40]. Amoozadeh *et al.* demonstrated that insider cyber-attacks could cause significant instability of CACC vehicle stream based on simulation, and then put forward several countermeasures [34]. In the aforementioned works, CACC is chosen as the only longitudinally automation control system for CAV simulations. Besides, Petit and Shladover did the first investigation of the potential cyber-attacks specific to automated vehicles with their special needs and vulnerabilities [3]. Jia *et al.* systematically conducted a survey on platoon-based vehicular cyber-physical systems [42]. Reilly *et al.* presented a controllability analysis of freeways with coordinated metering to evaluate impact of control system cyber-physical attacks [43]. Generally, much attention has been paid to the communication system and safety analysis, and thus the inherent characteristics of cyber-attack need further explorations. Also, more investigations should be conducted on its impact on traffic flow stability, efficiency, emissions and fuel consumption.

In this paper, we differentiate from the previous studies and emphatically address the following questions:

(1) What factors influence the traffic system under cyber-attack?

(2) What is the difference between cyber-attacks on position and speed?

(3) How sensitive is the traffic system to different cyber-attacked scenarios?

The remainder of this paper is structured as follows: Section II describes the methodology, including the evaluation framework for cyber-attacked traffic and simulation experiment designs. In Section III, the impact of important factors is analyzed, such as object of cyber-attack, proportion of cyber-attacked vehicles, cyber-attack severity. Section IV presents numerical simulation results to indicate the characteristics of the traffic flow under cyber-attack. Sensitivity analysis of cyber-attack range and traffic demand is conducted in Section V. Finally, some conclusions are summarized in Section VI.

II. METHODOLOGY

A. FRAMEWORK

The framework for evaluation of cyber-attack on traffic flow is shown in Fig. 1. It consists of four steps:

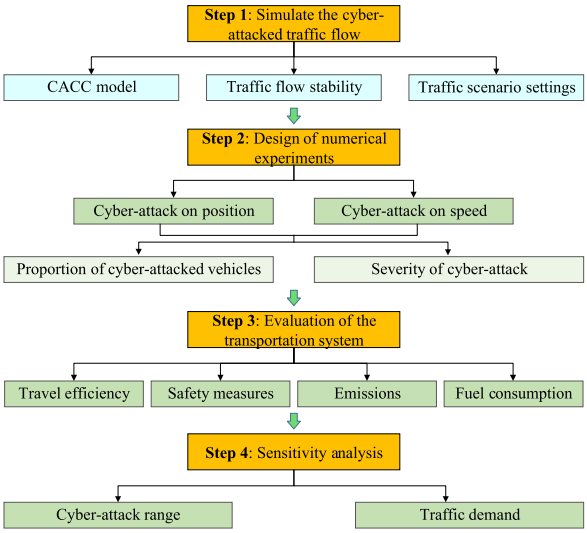

FIGURE 1. Framework of the study.

- **Step 1:** Model the cyber-attacked traffic flow. To simulate longitude control on CAVs, CACC model is used to characterize the car-following behaviors. Moreover, cyber-attack on traffic flow stability is analyzed from a theoretical prospective, and then traffic scenarios are designed to provide a basis for cyber-attack measurement.
- **Step 2**: Based on CACC model and analysis of traffic flow stability, the microscopic simulation testbed is established to imitate potential cyber-attacks on CAVs. Cyber-attacks on position and speed are respectively considered. Also, proportion of cyber-attacked vehicles and cyber-attack severity are selected as independent variables throughout the experiment.
- **Step 3**: Numerical simulations are conducted to display the performance of a basic freeway bottleneck in travel efficiency, traffic safety, emissions and fuel consumption.
- **Step 4**: Cyber-attack range and traffic demand are two important parameters, which the transportation system may be sensitive to. Therefore, sensitivity analysis is conducted to investigate their impact on simulation results.

B. TRAFFIC FLOW MODEL

It is well known that the technology of CACC is the most representative applied in CAVs' longitudinal control. The California Program on PATH developed a CACC car-following model and calibrated it using production cars equipped with PATH-Nissan High-Level Controller, which is one of few realistic models based on experimental data [13], [14], [17], [21], [22]. The CACC car-following model is expressed as follows:

$$v_{sv}(t) = v_{sv}(t - \Delta t) + k_p e_k(t) + k_d \dot{e}_k(t) \quad (1)$$

$$a_{sv}(t) = (v_{sv}(t) - v_{sv}(t - \Delta t))/\Delta t \quad (2)$$

$$x_{sv}(t) = x_{sv}(t - \Delta t) + v_{sv}(t)\Delta t \quad (3)$$

where v_{sv}, a_{sv} and x_{sv} are speed, acceleration and position of the subject vehicle, respectively. Δt is the time step. k_p and k_d are the model coefficients and gains for adjusting the time gap between the subject vehicle and the preceding vehicle. e_k is the time gap error and $\dot{e}_k$ is the derivative. They are described by the following:

$$e_k(t) = x_p(t-\Delta t) - x_{sv}(t-\Delta t) - t_{hw}v_{sv}(t-\Delta t) - L_{veh} \quad (4)$$

$$\dot{e}_k(t) = v_p(t-\Delta t) - v_{sv}(t-\Delta t) - t_{hw}a_{sv}(t-\Delta t) \quad (5)$$

where x_p and v_p are the position and speed of the preceding vehicle, respectively. L_{veh} is the vehicle length. t_{hw} is the desired time gap of the CACC controller. The units for distance, speed, acceleration and time are m, m/s, m/s^2 and s, respectively. According to the field tests, the parameters are calibrated as follows: $\Delta t = 0.01$ s, $t_{hw} = 0.6$ s, $k_p = 0.45$, $k_d = 0.25$.

C. CYBER-ATTACK ON TRAFFIC FLOW STABILITY

CACC is considered as a key enabling technology to automatically regulate the inter-vehicle distances in a vehicle platooning while maintaining the string stability. However, potential cyber-attack may have negative impact on the traffic flow stability [10], [19], [39], [41], [44]. In this case, the stability is theoretically investigated in terms of cyber-attacked position and speed. Similarly, the CACC model can be written as:

$$\dot{v} = \frac{k_p\,(h - s_0 - L_{veh} - t_{hw}v) + k_d\Delta v}{\Delta t + k_d t_{hw}} \quad (6)$$

where h denotes the space headway. Δv is the speed difference between the subject vehicle and the preceding one. The other parameters have the same meanings defined above. (6) can be written for the cyber-attacked condition:

$$f = \frac{k_p\,(\alpha h - s_0 - L_{veh} - t_{hw}v) + k_d\beta\Delta v}{\Delta t + k_d t_{hw}} \quad (7)$$

where f represents the general expression of traffic flow model. α and β denote the severity of cyber-attack on position and speed, respectively. Then, the three partial differentials of the model with respect to v, Δv, and h at the equilibrium state are presented as follows:

$$f^v = -\frac{k_p t_{hw}}{\Delta t + k_d t_{hw}} \quad (8)$$

$$f^{\Delta v} = \frac{\beta k_d}{\Delta t + k_d t_{hw}} \quad (9)$$

$$f^h = \frac{\alpha k_p}{\Delta t + k_d t_{hw}} \quad (10)$$

The value of stability condition F reflects the general instability condition of car-following model with the acceleration function, and it is calculated as (11). The proof follows the Lyapnuov stability theory and hence is omitted. The readers can refer to Wilsoon [44] for a complete proof.

$$F = \frac{1}{2}\left(f^v\right)^2 - f^v f^{\Delta v} - f^h \quad (11)$$

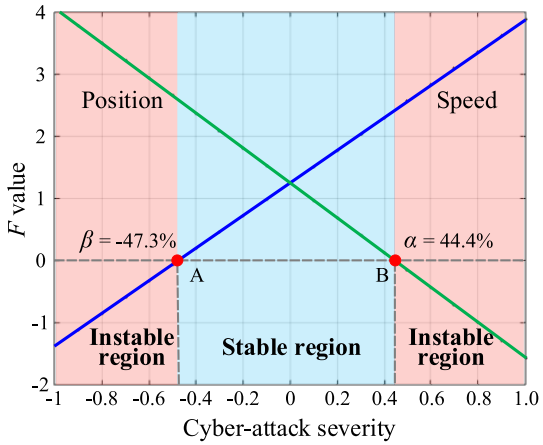

FIGURE 2. Impact of cyber-attack on traffic flow stability.

The traffic flow is instable if the following equation holds.

$$F < 0 \quad (12)$$

During numerical simulation, the value of α and β is set to range from 0 to 2, and the result of stability in cyber-attacked traffic is shown in Fig. 2.

In Fig. 2, the coordinate origin of x-axis denotes no cyber-attack. Obviously, the distribution map is divided into three parts and the middle part represents stable region both for position- and speed-attacked scenarios. Specifically, the stability condition of the CACC model holds when the term of speed is cyber-attacked by 47.3%. In this case, the subject vehicle has little space to avoid rear-end collision because of fake information collected from the leading CAV. For the position, if it is overestimated by over 44.4%, the traffic flow starts to become unstable. Therefore, underestimation of speed or overestimation of position can lead to traffic flow instability, and the lower value 44.4% is taken as the threshold. This is the reason why the value of cyber-attack severity is below the threshold during following experiments.

D. SIMULATION EXPERIMENT DESIGN

The topology structure of communications between CAVs under or without cyber-attacks is expressed in Fig. 3(a). If one CAV is under cyber-attack, it will transmit imprecise data to the following vehicle. In this case, we need to answer three important problems:

(1) How many CAVs are attacked?

(2) What is the quantitative index of cyber-attack severity?

(3) When or where do the cyber-attacks on CAVs start and finish?

For the first issue, we test different proportions of vehicles under cyber-attack and evaluate their impacts on traffic flow. Besides, another relevant variable is traffic demand, which is analyzed at the end of Section V. To handle the second problem, we define the fluctuation ratio of position or speed as cyber-attack severity. For example, if the speed of the subject vehicle is 20 m/s and the received imprecise information by the following vehicle is 16 m/s, the current

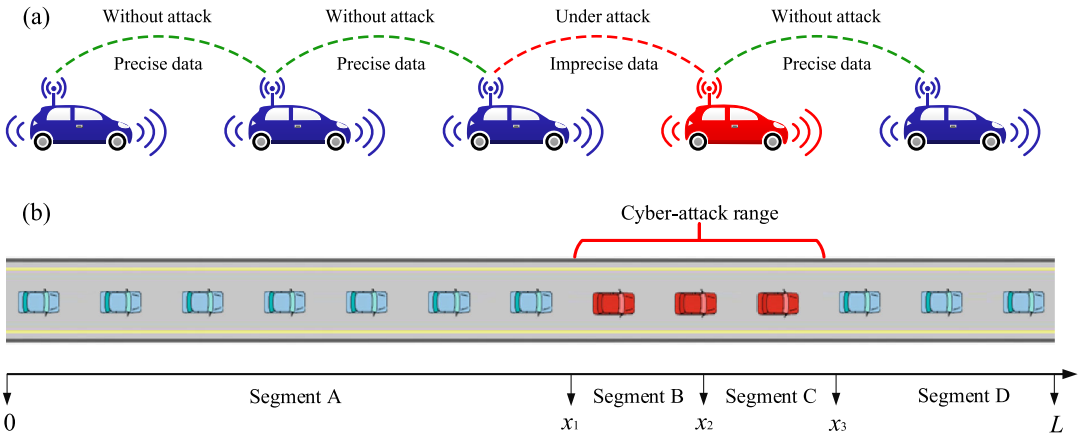

FIGURE 3. Schematic illustration of the study environment. (a) Communications between CAVs under or without cyber-attacks, and (b) traffic scenario and its coordinate system.

cyber-attack severity is 20%. Because each road-side unit is responsible for information transmission within a fixed area, a CAV which enters the cyber-attack area has a chance to be attacked, as shown in Fig. 3(b). Segment A and D are without cyber-attacks, while Segment B and C are cyber-attack areas. We assume that positions and speeds of CAVs in Segment A and D are iterated only by the car-following model. Correspondingly, those in Segment B and C fluctuate randomly at a certain severity, i.e. 0.1%, 0.5%, 1%, 2%, 4%, 8%, 16%, 32%. According to the findings in Fig. 2, the specific value of cyber-attack severity ranges from -44.4% to 44.4%, which ensures the traffic flow stability. For example, if the severity is set to 8%, the speed or position will be either over-or underestimated by 8%.

During simulations, Segment B and C are decided by x_1, x_2 and x_3. x_2 is the central position of attack range and it is a constant 1300 m. The interval of $[x_1, x_2]$ identically equals to $[x_2, x_3]$. Therefore, we can easily control the attack range by changing radius of $[x_1, x_3]$ during each experiment. The radius of attack range is limited by technology development in communication. In this paper, 300 m, 500 m and 700 m are chosen to represent different levels of communication technology [13], [45]. The default value 300 m reflects the current level.

For the other parameter settings, the ranges of speed and acceleration are [0, 30 m/s] and [-4 m/s^2, 2 m/s^2], respectively. In addition, the lengths of road and vehicle are $L = 3000$ m and $L_{veh} = 5$ m. Each simulation period is 1 h, and we repeat 10 times for average results to reduce the random errors.

III. EVALUATION INDEX

A. ROAD CAPACITY

The pipeline capacity is defined as the maximum 15-minute moving average flow rate observed upstream the cyber-attacked flow. In this paper, the measurement point for road capacity is chosen at $x = 2500$ m in Fig. 3(b). The experiments begin with simulating a constant and relatively low traffic volume for one hour. If the freeway remains free-flowing, then subsequent simulations are conducted with slightly higher volume input (e.g., plus 1000 veh/h), until the highest observed 15-minute moving average flow no longer increases as the input became larger [21]. The capacity is finally determined based on 10 replications with different random seeds.

$$C = q_{15\,\mathrm{min}} \times 4 \tag{13}$$

where C is road capacity and $q_{15\mathrm{min}}$ is the highest 15-minute flow.

B. SURROGATE SAFETY MEASURE

Rear-end collision risk indexes (RCRI) establish relation between longitudinal safety and vehicle dynamic trajectory data. Previously, various indexes have been proposed and extensively applied [15], [46]. In this study, we utilize a RCRI based on safe stopping distance, which has been widely used in previous researches [4], [11], [20], [47], [48].

Assume that the preceding vehicle takes an emergency stopping maneuver with the maximum deceleration rate. The subject vehicle has to react and brake to avoid a collision. If the stopping distance of the preceding vehicle is larger than that of the subject vehicle, it is safe; otherwise it is dangerous. Fig. 4 illustrates the safe stopping distance.

Specifically, the RCRI index based on safe stopping distances is calculated as follows:

$$SSDp = h + \frac{v_p^2}{2dm} \tag{14}$$

$$SSDsv = vsvtd + \frac{v_{sv}^2}{2dm} \tag{15}$$

$$RCRI = \begin{cases} 0 & if\ SSDp > SSDsv \\ 1 & otherwise \end{cases} \tag{16}$$

$$MRCRI = \frac{\sum_{t=1}^{T}\sum_{i=1}^{N} RCRI}{\sum_{t=1}^{T}\sum_{i=1}^{N} flag} \tag{17}$$

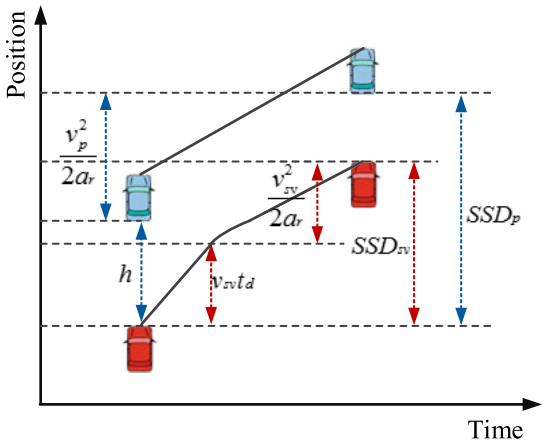

FIGURE 4. Rear-end collision risk index.

TABLE 1. Rear-end collision risk criteria.

Level	M_{RCRI} range	Level	M_{RCRI} range
A	(0, 0.251)	B	(0.251, 0.306)
C	(0.306, 0.355)	D	(0.355, 0.416)
E	(0.416, 0.510)	F	(0.510, 1)

where SSD_p and SSD_{sv} are safe stopping distances of the preceding and subject vehicles, respectively. d_m is the deceleration rate and t_d is the time delay. In this study, a deceleration rate of 3.4 m/s^2 is adopted and a time delay of 0.1 s is used for CAVs according to previous studies [6], [17]. T is the total time and N is the total vehicles. *flag* is used as the mark of number. M_{RCRI} is the average RCRI of all space-time points.

Rear-end collision risk criteria for freeway safety can be stated in terms of the average RCRI, as shown in Table 1 [46]. The clustering results are based on a tremendous amount of data investigated from freeways.

On the one hand, Level A is considered to be very safe traffic conditions with low M_{RCRI}. On the other hand, Level F would describe the traffic at the highest risk on freeway when M_{RCRI} exceeds 0.510. Besides, CAVs may choose continuous emergency braking operations under this level, and such unsafe traffic conditions can lead to the highest possibility of subsequent accident occurrences.

C. EMISSION AND FUEL CONSUMPTION

Table 2 lists emission and fuel consumption rates for general cars under four typical traffic conditions [49]. There are relatively small differences between HC, NO_X, CO_2, and fuel consumption under three conditions, including free flow, transition and congestion. Compared with the other three conditions, work zone shows the lowest emission rates for HC, CO, and NO_X. On the contrary, the lower speed in work zone brings about higher CO_2 emissions and fuel consumption.

The formula for calculating emissions and fuel consumption is as

$$M = \int_0^L f(v)dx \tag{18}$$

TABLE 2. Summary of emission factors and fuel consumption rates.

Traffic Condition	Speed (km/h)	Emission Factors (g/km)				Fuel Consumption (g/km)
		HC	CO	NO_x	CO_2	
Free flow	112	0.08	4.09	0.21	178	60
Transition	101	0.09	5.03	0.22	180	62
Congestion	90	0.08	4.27	0.21	182	63
Work zone	33	0.04	1.32	0.13	211	67

where M denotes the weight of a certain emission or fuel consumption. It is an integral of a function from the starting point to the ending of the road. L is the road length and $f(v)$ is a function of speed, which can be obtained in Table 2. Because there are only four discrete values for estimation, a linear interpolation of the speed within the range is applied to calculate the total weight of emissions and fuel consumption. In addition, if the speed exceeds the maximum or minimum threshold, an effective and convenient solution is taking on the boundary value.

IV. NUMERICAL SIMULATION RESULTS

In this section, we design extensive numerical simulations to evaluate impacts of cyber-attacks on traffic flow composed of all CAVs. P, S, R and Q, which respectively stand for proportion of attacked vehicles, cyber-attack severity, cyber-attack range and traffic demand, are selected as study objects. Their influences on the traffic system are tested to predict potential cyber-attacked scenarios in the future, i.e., efficiency, safety, emission and fuel consumption.

A. TRAVEL EFFICIENCY

We first investigate the impacts of proportion of vehicles attacked on positions, as shown in Fig. 5. The proportion P varies from 0 to 100% with 20-percentage intervals. The other parameters are set as follows: $S = 2\%$, $R = 300$ m and $Q = 1000$ vehicles per hour (vph).

Obviously, with the increase of proportion of attacked vehicle, the average speed decreases gradually, especially in the cyber-attack area. When the proportion is less than 60%, CAVs travel along the road at almost free-flow speeds. The slight congestions caused by speed drop behaviors exist only in a short-range section from 1000 m to 1600 m. Such an oscillatory jam always lasts for several minutes until the next jam is observed. However, when the proportion increases to 60% or a higher percentage, CAVs in the cyber-attack area start to slow down, and this delay triggers heavier congestions caused by position fluctuations. Each oscillatory jam tends to be close to the next one and gather into a mass. Then, deceleration movements become more frequent. Meanwhile, the phenomenon of speed reduction is more and more evident, as presented in Fig. 5(d)-(f). It is worth noting that the congestions in Fig. 5(f) are much heavier than the others. On the one hand, the yellow and red color lumps indicate significant speed drops, which result in queues and delay. On the other hand, the severe congestions propagate upstream

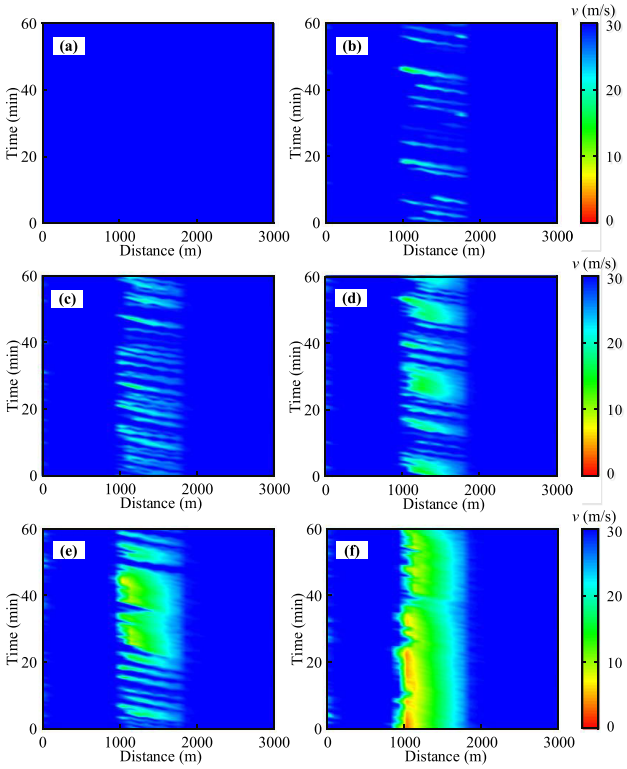

FIGURE 5. Spatiotemporal dynamics of average speed with position attacked. (a) $P = 0$, as a reference group, (b) $P = 20\%$, (c) $P = 40\%$, (d) $P = 60\%$, (e) $P = 80\%$, and (f) $P = 100\%$.

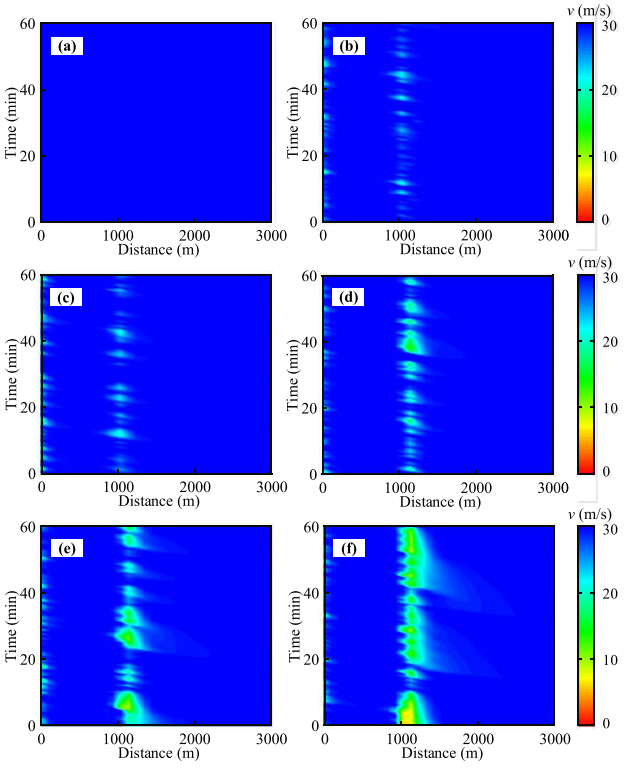

FIGURE 6. Spatiotemporal dynamics of average speed with speed attacked. (a) $P = 0$, as a reference group, (b) $P = 20\%$, (c) $P = 40\%$, (d) $P = 60\%$, (e) $P = 80\%$, and (f) $P = 100\%$.

with a certain speed, and the influence area even exceeds 1000 m. From this point of view, practical suggestions for freeway control and management are enforcing anti-cyber-attack abilities and making sure less vehicles under attack if it is unavoidable.

The similar experiments are conducted on the traffic scenario with speed attacked, as shown in Fig. 6. It is obvious that vehicles keep a high speed when the proportion of attacked vehicles is less than 80% during the whole simulations. Even though the proportion rises to 80%, the congestions caused by attacked speeds are still rare and dissipate quickly in a short time. When the proportion is 100%, the congestions form upstream of the cyber-attack area and have few negative effects on its downstream area. Notice that the average speeds of CAVs in the severest congestions are approximately 10 m/s, as shown in Fig. 6(f), which leads to relatively less delay than other conditions (Fig. 5(d)-(f)). Generally, from the perspective of influence area, the range of speed reduction by cyber-attack is around [1000 m, 1300 m]. Compared with the position-attacked traffic, the scenario with the same proportion of speed-attacked vehicles performs much better both in speed drops and influence area of congestions.

Table 3 presents the impacts of cyber-attack severity and proportion of attacked vehicles on speeds. It is apparent that with the increase of severity, the average speeds decrease remarkably when the CAVs' positions are attacked. On the contrary, the amplitudes of oscillation in average speeds under speed-attacked conditions are much smaller, especially with small proportions of attacked vehicles. In terms of specific values, the speed ranges of the traffic attacked on speed are nearly between one-fourth and one-third of that under position-attacked conditions. For instance, the best case is the condition with the lowest severity and the smallest proportion of attacked vehicles. And then, the speed ranges for position- and speed-attacked traffic are -2.25% and -0.81%, where the latter is approximately one-third of the former. In addition, the biggest change of position-attacked traffic is over -55% while that is less than -20% with speed attacked among all conditions summarized in Table 3. So, it is a quantitative proof that the transport system controlled by CACC has an inherent function of defending cyber-attacks on speed.

Fig. 7 shows the road capacity changes with proportion of cyber-attacked vehicles and cyber-attack severity. The severity level is 2% in Fig. 7(a) and 50% of vehicles on are considered to be cyber-attacked in Fig. 7(b). Basically, the capacity keeps dropping when more vehicles are cyber-attacked or the severity becomes higher. However, the difference in the traffic scenarios with cyber-attacked position and speed can be clearly observed. Specifically, the traffic reaches higher capacity if the speed is on cyber-attack, and the jerk tends to be zero when the proportion of cyber-attacked vehicles is over 60%, as shown in Fig. 7(a). However, during the investigation of cyber-attack severity in Fig. 7(b), two values of the jerk are both positive, which indicates that the transportation system

TABLE 3. Statistics summary of speed reductions caused by cyber-attacks on position and speed. Six values of cyber-attack severity and three proportions of attacked vehicles are selected to evaluate the impacts on speeds. The reference group is the stable traffic flow without cyber-attack.

Type	P	S (%)					
		0.1	0.5	2	8	16	32
Position	20	-2.25%	-4.37%	-6.71%	-10.93%	-15.14%	-19.31%
	60	-3.92%	-8.11%	-11.42%	-17.45%	-26.50%	-37.68%
	100	-6.14%	-12.86%	-19.65%	-28.76%	-40.25%	-55.89%
Speed	20	-0.81%	-1.59%	-2.30%	-3.04%	-4.35%	-5.66%
	60	-1.16%	-2.17%	-3.22%	-4.87%	-6.76%	-8.87%
	100	-2.58%	-3.92%	-5.16%	-7.35%	-11.48%	-18.59%

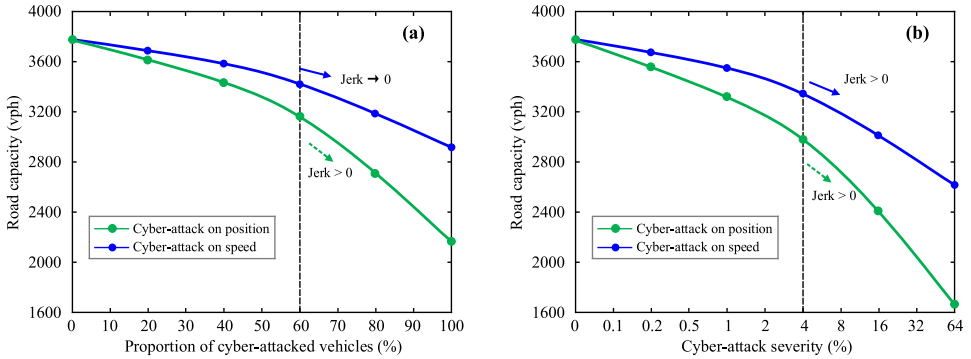

FIGURE 7. Impact of cyber-attack on road capacity.

TABLE 4. Changes of risky RCRI.

P (%)	S (%)					
	0.1	0.5	2	8	16	32
0	1.0	1.0	1.0	1.0	1.0	1.0
10	4.4	21.7	31.7	42.8	45.9	50.1
20	6.8	31.2	42.6	51.2	53.2	59.5
30	9.3	37.1	48.9	57.3	59.2	63.6
40	11.8	43.3	53.3	61.1	64.5	66.9
50	14.5	48.6	58.0	63.0	67.4	70.3
60	17.3	51.5	60.4	67.0	70.2	73.3
70	20.1	54.1	61.8	68.9	72.1	75.8
80	22.4	55.5	62.8	70.0	73.4	76.9
90	25.0	56.2	64.1	71.2	74.7	78.1
100	27.5	57.3	65.6	72.5	76.1	79.4

is more sensitive to the severity, especially when its value exceeds 4%.

B. SAFETY ANALYSIS

Taking the position-attacked scenario with 0.1% severity as reference group, changes of risky RCRI are summarized in Table 4. With the increase of severity, cyber-attack produces at least a 4-fold decrease in terms of RCRI when there is only 10% of vehicles are cyber-attacked. If all CAVs are on cyber-attack, changes of risky RCRI range from 27.5 to 79.4 times when cyber-attack severity increases from 0.1% to 32%. Generally, the higher the cyber-attack severity, the worse the traffic condition. Similarly, more attacked vehicles inevitably cause the serious deterioration of safety condition. For example, the cyber-attack severity increases to 0.5% or more and the proportion of cyber-attacked vehicles reaches 60%, the times of RCRI changes are all more than 50 in comparison with the reference group.

Based on RCRI values, the evaluation of safety level is distributed in Fig. 8. Cyber-attack severity is tested from 0 to 32%, as shown on the abscissa axis. The average safety levels of all CAVs with cyber-attacked position are summarized in Fig. 8(a), and Fig. 8(b) presents the traffic condition only under speed-attack. The most intuitive performance is that Level E/F is observed with high-proportion of cyber-attack vehicles and high-level severity, since more attacked CAVs with high-level severity result in lower speeds. In this case, the following vehicles has less time to react in response to sudden deceleration of preceding vehicles. Fortunately, the traffic is still at lower risk, and safety level remains A in speed-attack scenarios, as shown in Fig. 8(b). Additionally, safety of the worst condition is assessed as Level C. It may be an acceptable result because of rare accidents under C-level driving conditions.

Moreover, the critical value of cyber-attack severity for position is around 0.5% while 8% for speed. It is also directly proved that the transport system is much more sensitive to cyber-attacks on position than speed, which is consistent with the above findings. For example, when the proportion of attacked vehicles is 50% and the cyber-attack severity is 8%, average safety levels of the traffic under position and speed attacks are approximately C and A, respectively. In regard to the ordinate axis, boundary points for the two scenarios are $P = 40\%$ and $P = 70\%$, which are similar to the phenomena drawn in Fig. 5 and Fig. 6. Moreover, the safety

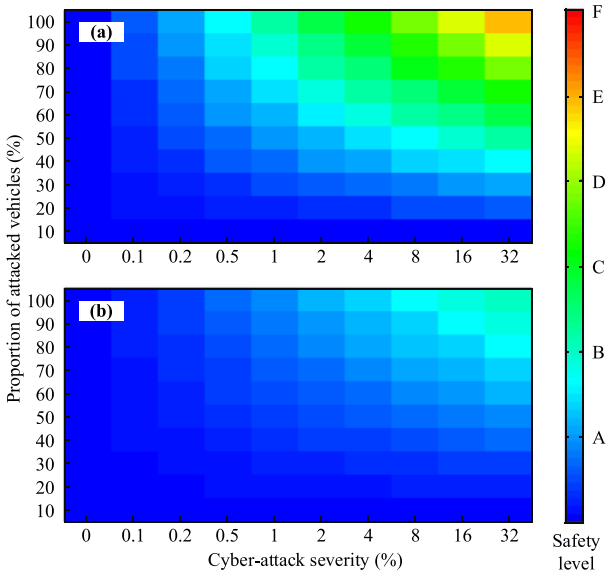

FIGURE 8. Impact of cyber-attack on safety level.

TABLE 5. Summary of pollutant emissions and fuel consumption.

Type	Rate (%)	Emission Factors (g/veh)					Fuel consumption (g/veh)
		HC	CO	NO_x	CO_2	Sum	
P	20	0.21	12.86	0.58	524	537.65	189.54
	40	0.22	13.51	0.60	535	549.33	191.70
	60	0.20	12.26	0.56	538	551.02	193.96
	80	0.17	9.76	0.51	559	569.44	197.12
	100	0.13	5.43	0.45	602	608.01	198.31
S	0.1	0.20	12.65	0.56	533	546.41	188.83
	0.5	0.22	14.13	0.61	551	565.96	192.05
	2	0.19	13.22	0.56	562	575.97	194.33
	8	0.16	10.51	0.51	570	581.18	196.78
	16	0.15	6.23	0.48	592	598.86	198.91
	32	0.12	4.87	0.44	611	616.43	200.22

levels in Fig. 8(b) rise rather less than that in Fig. 8(a) with the same amplitude in proportion of attacked vehicles.

C. RESULTS OF EMISSIONS AND FUEL CONSUMPTION

Nowadays, there is no doubt that traffic-related pollutants have direct impact on the globe climate and public health. Table 5 shows four main pollutants emitted by vehicles and fuel consumptions in 11 groups of traffic scenarios. Although tiny differences of emission rates are observed in Table 2, the total emission of four pollutants and fuel consumption keep monotonically decreasing during one type of experiments. The scenarios designed for various proportions of cyber-attack vehicles have a similar trend to that with different cyber-attack severities.

Specifically, emissions of HC and NO_x are less than 1 g/veh while the mass CO_2 is always more than 520 g/veh. So, CO_2 is absolutely the main pollutant of vehicles. From the perspective of sum, the emission is increased by 70 g/veh when the proportion of cyber-attacked vehicles rises from 20% to 100%. The same phenomena can be observed in

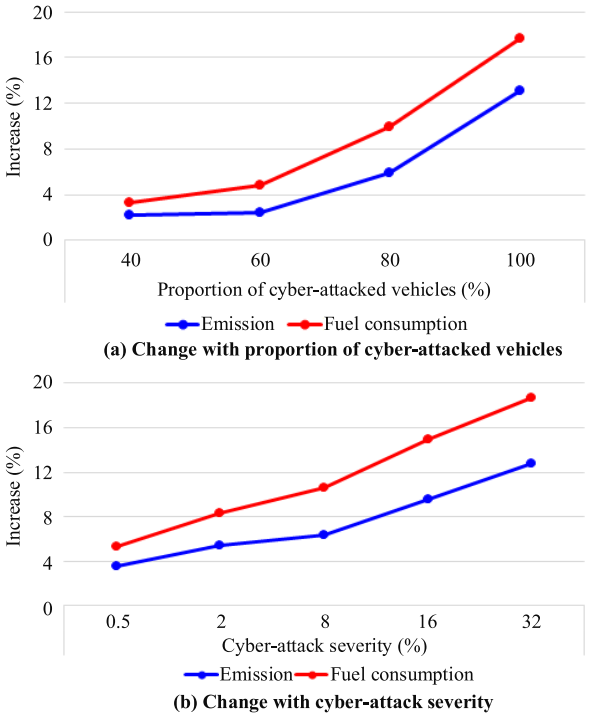

FIGURE 9. Cyber-attack impact on emission and fuel consumption.

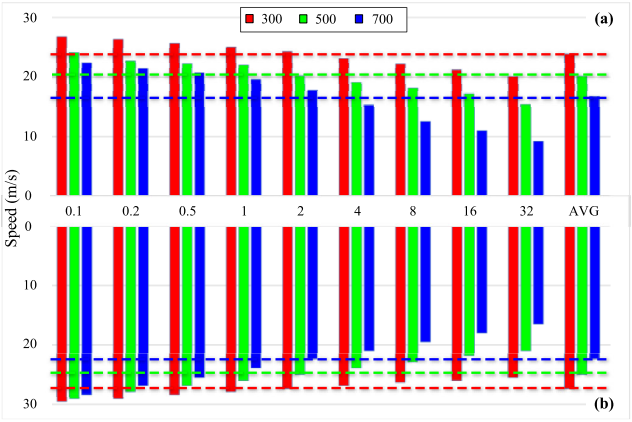

FIGURE 10. Impact of cyber-attack range on average speeds. (a) Cyber-attacks on positions, and (b) cyber-attacks on speeds. AVG on the abscissa axis stands for average, and each of the three horizontal lines in the sub-graphs represents the average level.

the test for cyber-attack severity. However, only 10 g/veh fuel consumption compensates for cyber-attack. For example, the fuel consumption increases from 189.54 g/veh to 198.31 g/veh when the proportion of cyber-attacked vehicles is increased by 80%. The gap for fuel consumptions in two traffic scenarios is only 8.77 g/veh. Therefore, the transportation system still maintains relatively stable performance in total emissions and fuel consumption, although cyber-attack has negative but limited impact on these indexes.

To this end, further investigations are conducted to assess the changes of emissions and fuel consumption due to cyber-attack. As shown in Fig. 9, whether the cyber-attack occurs on position or speed, the magnitudes of increase are generally

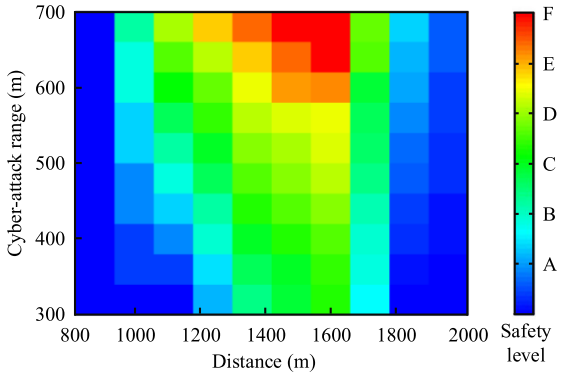

FIGURE 11. Distribution of safety level along the roadway.

below 20%. Obviously, changes of fuel consumption increase faster than emissions, meanwhile the gap widens gradually. Additionally, the maximum increases of fuel consumption exceed 16% both in the tests for two separate groups. In contrast, there is a 2%-13% increase during emission evaluation. Compared with the values of proportion of cyber-attacked vehicles P and cyber-attack severity S, the magnitudes of increase in emissions and fuel consumption are relatively smaller.

V. SENSITIVITY ANALYSIS

Sensitivity analysis is provided to study the effect of the parameters on simulation results. The parameters include cyber-attack range and traffic demand, which may affect both efficiency and safety of the transportation system. So, it needs a further exploration. Emissions and fuel consumption are not chosen as evaluation indexes in this section because the magnitude of changes caused by cyber-attack range and traffic demand is stably less than 20%, which is proved by the above experiments.

A. CYBER-ATTACK RANGE

Signal transmission is one of core technologies in the CAV industry, and the transmission range for communications between CAVs is the key performance indicator. We assume that if one road-side unit is cyber-attacked, there is a possibility of being attacked for all CAVs within the transmission range. On this basis, cyber-attack ranges are equal to the transmission distances. Three typical values are chosen to evaluate the impacts of cyber-attack range on average speeds, as shown in Fig. 10. They respectively represent the current, short-term and long-term levels in transmission technology.

Based on the above simulation results, we can draw several conclusions. Firstly, the longer the cyber-attack range, the lower the average speeds. It is interesting that improvement in transmission technology results in more negative effects on travel efficiency. Because long transmission distance leads to a large amount of CAVs under attack, it is reasonable that the average speeds decrease with the increase of cyber-attack range. Secondly, the traffic flow is more sensitive to the attacked position than speed, which is consistent with the above-mentioned experiments. Judging from the average level, CAVs in speed-attacked traffic are faster than that in position-attacked by 5 m/s-10 m/s. This is a big advantage in traffic efficiency and transport economy in terms of saving time. So, from a long-term perspective, improving the security of signal transmission becomes more vital in the future. Thirdly, the critical severity for distinguishing the speeds from the average is different from each other. Taking Fig. 10(a) as an example, we can easily find that the maximum severity of speeds below average for three traffic scenarios with different cyber-attack ranges is 2%, 2% and 4%, respectively. Therefore, avoiding severe cyber-attack on traffic flow becomes highly important when advanced communication technologies help more CAVs improve cooperation within a longer transmission range.

Identifying unsafe areas provides theoretical guidance for the management of automated highway systems in the foreseeable future. Fig. 11 shows the distribution of safety level along the influence area [800 m, 2000 m]. For each scenario, there is a noticeable difference between Level A and F. Specifically, safety level A is normally distributed upstream or downstream the bottleneck, while safety level F is centralized in the middle part with over 500-meter cyber-attack ranges ranged from 900 m to 1900 m. On the one hand, longer cyber-attack ranges directly lead to risky driving condition because it can bring about shorter time or space headway for the following vehicles and cause potential rear-end collisions in the same lane. On the other hand, it also avoids providing enough room for congestion dissipation and makes the driving situation worse over a longer period.

For each scenario with the same cyber-attack range, safety level shows a moderate decrease after a fast increase, and reaches the peak around $x = 1500$ m. From the perspective of location, the driving condition becomes more and more risky, and still maintains the momentum of worsening. Therefore, some control methods like VSL can be applied along the influence area for enough reaction time. Additionally, road-side units may send warning massages to CAVs and remind drivers to keep safe distance if allowed. From this point of view, traditional control technologies are a necessary complement for emergencies in the foreseeable transportation systems.

B. TRAFFIC DEMAND

With the popularity of CAVs, the increasing traffic demand will bring great pressure on transport system. In this section, we focus on the impact of traffic demand on travel efficiency and safety. For the sake of brevity, experiment results of position-attacked scenarios are only presented.

As shown in Fig. 12, with the increase of traffic demand from 1000 vph to 2000 vph, the average speeds decrease over 10 m/s under the same cyber-attack severity. The similar conclusion can be made if the cyber-attack severity is treated as independent variable. Specifically, all speeds in Fig. 12(a) are over 20 m/s while those are below 20 m/s in Fig. 12(c). Moreover, with the same increase of 500 vph, the 2000-vph

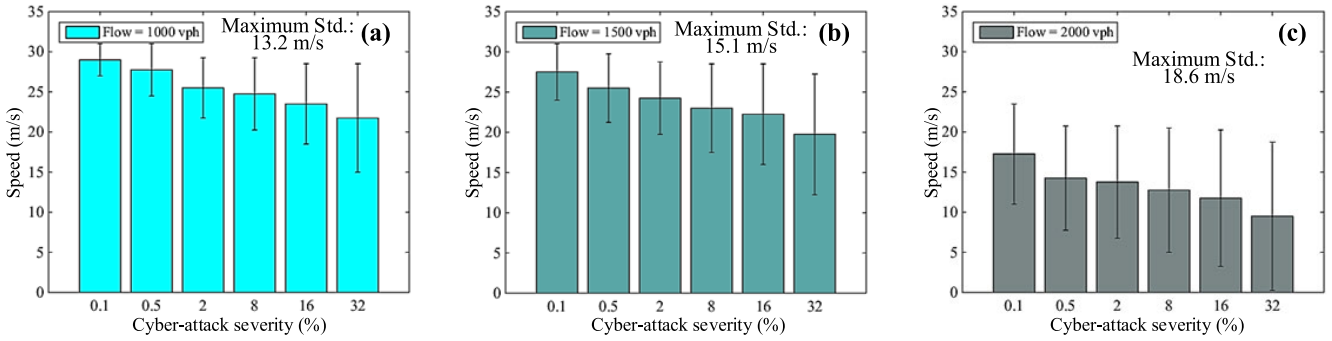

FIGURE 12. Characteristics of average speed and standard deviation versus traffic demand and cyber-attack severity. (a) Q = 1000 vph, (b) Q = 1500 vph, and (c) Q = 2000 vph.

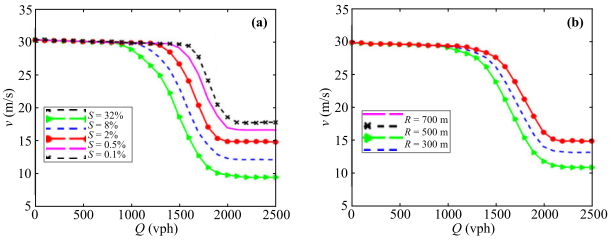

FIGURE 13. Impact of cyber-attack severity and range on speed with different traffic demands. (a) 5 values of cyber-attack severity are chosen, i.e. 0.1%, 0.5%, 2%, 8%, 32%. (b) Three typical radiuses of cyber-attack range are selected, including 300 m, 500 m and 700 m.

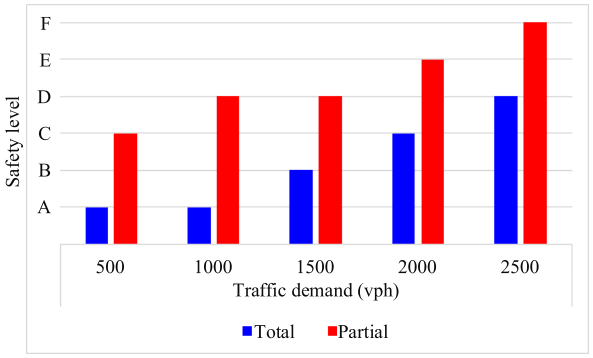

FIGURE 14. Safety evaluation in various traffic demands.

traffic performs much worse than the 1500-vph one according to the serious decline in speed. It explains that a large number of CAVs on the road are a big threat to traffic safety, and route guidance in advance is an effective measure to avoid the phenomenon. In addition, the trend of standard deviation of speed is same as the average. The maximum standard deviation reaches 18.6 m/s and is nearly equal to the average, as shown in Fig. 12(c). And thus, the big fluctuations in speed caused by cyber-attack appear frequently, which can reduce travel efficiency and traffic safety.

In order to imitate the real world, the experiments with consecutive traffic demand are conducted versus cyber-attack severity and range. As shown in Fig. 13, the lines for each scenario can be divided into three sections. First, the trend line of speed shows an approximately linear decreasing relationship with the flow before dropping, where the traffic still can be considered as the free flow. Second, the speeds drop sharply with the increase of traffic demand owing to the high-frequency cyber-attacks on CAVs. Ultimately, the average speeds all tend to reach a certain constant value. It's remarkable that the sensitive traffic demand always lies within the range [1000 vph, 2000 vph], where marginal utility is diminishing. What's more, the jam speeds in Fig. 13(a) range from 10 m/s to 18 m/s while the speed drop is only 4 m/s in Fig. 13(b). Therefore, compared with cyber-attack range, the severity should attract more attention from road administrators, and be controlled within a certain level if it happens.

The traffic demand is set to vary from 500 vph to 2500 vph with a 500-vph interval. Fig. 14 illustrates the safety level for five scenarios. The total and partial results respectively represent the whole road and the influence area [800 m, 2000 m]. Generally, the total road has at least two levels ahead of the partial. The safest level is A for the total while C for the partial. Moreover, the safety of the partial road is deteriorated to Level F when the traffic demand increases to 2500 vph. So, it should account for the high safety level of the total road, which indicates that solving local problems can improve safety the performance of overall situation.

VI. CONCLUSION

In this paper, we first design the traffic flow simulation experiment for cyber-attacks on CAVs, and then analyze impact of the proportion of attacked vehicles, cyber-attack severity, cyber-attack range and traffic demand. According to the performance on efficiency, safety, emissions and fuel consumption under different traffic conditions, the major results are concluded as follows:

(1) Traffic congestions occur frequently and have significant negative effects on the cyber-attack area when the proportion of attacked vehicles are over 60% under position-attacked conditions. In contrast, the speed-attacked traffic is not sensitive to the proportion of attacked vehicles. The critical values of cyber-attack severity for the position- and speed-attacked traffic are respectively 1% and 8%, from which the speeds decline dramatically. Compared with the stable traffic without cyber-attack, the decreases in average speed under speed-attacked conditions are nearly between one-fourth and one-third of that with attacked positions.

(2) In the influence area caused by cyber-attack, the safety condition gets worse and leads 2-3 levels than the whole road, especially in the position-attacked scenarios. Moreover, cyber-attack causes more 2-20% emissions and fuel consumption with the increase of cyber-attacked vehicles and cyber-attack severity.

(3) The longer cyber-attack range caused by the improvement of transmission technology results in more negative effects on traffic efficiency and safety. The average speeds approximately drop by 5 m/s with a 200-meter increase of cyber-attack range.

(4) Compared with the traffic below 1500 vph, the 2000-vph traffic demand results in striking decreases and big fluctuations in speeds. In addition, [1000 vph, 2000 vph] is the sensitive range for traffic demand management, where route guidance in advance may be necessary.

(5) From the view of attackers, vehicle's position may be the most potential attack target, and its severity over 1% can cause significant negative effects on travel efficiency and traffic safety. For the defenders, some control methods like VSL can be applied along the influence area for enough reaction time. Additionally, road-side units may send warning massages to CAVs and remind drivers to keep safe distance if unknown attack occurs. There, if the security cannot be guaranteed completely, the control right of CAV should be controlled by the driver to support emergency response.

In our future work, the following aspects need special attention: (1) This study only focuses on one-lane road, and hence, other types of highway shall be analyzed in future research, including on-ramps and off-ramps. (2) The traffic system contains many variables. Future research could investigate the scenarios that both positions and speeds are attacked. (3) Lane-changings are a common phenomenon in the realistic world, and further research is required to explore impacts of lane-changings on the cyber-attacked traffic system.

REFERENCES

[1] C. Dong, H. Wang, Y. Li, W. Wang, and Z. Zhang, "Route control strategies for autonomous vehicles exiting to off-ramps," *IEEE Trans. Intell. Transp. Syst.*, early access, Jul. 10, 2019, doi: 10.1109/TITS.2019.2925319.

[2] D. Ni, "Determining traffic-flow characteristics by definition for application in ITS," *IEEE Trans. Intell. Transp. Syst.*, vol. 8, no. 2, pp. 181–187, Jun. 2007.

[3] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.

[4] C. Dong, H. Wang, Q. Chen, D. Ni, and Y. Li, "Simulation-based assessment of multilane separate freeways at toll station area: A case study from huludao toll station on shenshan freeway," *Sustainability*, vol. 11, no. 11, p. 3057, 2019.

[5] C. Wang, C. C. Xu, J. X. Xia, Z. D. Qian, and L. J. Lu, "A combined use of microscopic traffic simulation and extreme value methods for traffic safety evaluation," *Transp. Res. Part C Emerg. Technol.*, vol. 90, pp. 281–291, May 2018.

[6] Y. Li, H. Wang, W. Wang, L. Xing, S. Liu, and X. Wei, "Evaluation of the impacts of cooperative adaptive cruise control on reducing rear-end collision risks on freeways," *Accident Anal. Prevention*, vol. 98, pp. 87–95, Jan. 2017.

[7] D. Ni, J. D. Leonard, C. Jia, and J. Wang, "Vehicle longitudinal control and traffic stream modeling," *Transp. Sci.*, vol. 50, no. 3, pp. 1016–1031, Aug. 2016.

[8] F. Chen and S. Chen, "Injury severities of truck drivers in single- and multi-vehicle accidents on rural highways," *Accident Anal. Prevention*, vol. 43, no. 5, pp. 1677–1688, Sep. 2011.

[9] Y. Li, Z. Li, H. Wang, W. Wang, and L. Xing, "Evaluating the safety impact of adaptive cruise control in traffic oscillations on freeways," *Accident Anal. Prevention*, vol. 104, pp. 137–145, Jul. 2017.

[10] Y. Guo, Z. Li, P. Liu, and Y. Wu, "Modeling correlation and heterogeneity in crash rates by collision types using full Bayesian random parameters multivariate tobit model," *Accident Anal. Prevention*, vol. 128, pp. 164–174, Jul. 2019.

[11] Y.-Y. Qin, Z.-Y. He, and B. Ran, "Rear-end crash risk of CACC-manual driven mixed flow considering the degeneration of CACC systems," *IEEE Access*, vol. 7, pp. 140421–140429, 2019.

[12] C. Xu, J. Ji, and P. Liu, "The station-free sharing bike demand forecasting with a deep learning approach and large-scale datasets," *Transp. Res. C, Emerg. Technol.*, vol. 95, pp. 47–60, Oct. 2018.

[13] C. Dong, H. Wang, Y. Li, Y. Liu, and Q. Chen, "Economic comparison between vehicle-to-vehicle (V2 V) and vehicle-to-infrastructure (V2I) at freeway on-ramps based on microscopic simulations," *IET Intell. Transp. Syst.*, vol. 13, no. 11, pp. 1726–1735, Nov. 2019.

[14] Y. Li, Y. Tu, Q. Fan, C. Dong, and W. Wang, "Influence of cyber-attacks on longitudinal safety of connected and automated vehicles," *Accident Anal. Prevention*, vol. 121, pp. 148–156, Dec. 2018.

[15] Y. Li, H. Wang, W. Wang, S. Liu, and Y. Xiang, "Reducing the risk of rear-end collisions with infrastructure-to-vehicle (I2 V) integration of variable speed limit control and adaptive cruise control system," *Traffic Injury Prevention*, vol. 17, no. 6, pp. 597–603, Aug. 2016.

[16] Y. Li, C. Xu, L. Xing, and W. Wang, "Integrated cooperative adaptive cruise and variable speed limit controls for reducing rear-end collision risks near freeway bottlenecks based on micro-simulations," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 3157–3167, Nov. 2017.

[17] S. E. Shladover, C. Nowakowski, X.-Y. Lu, and R. Ferlis, "Cooperative adaptive cruise control: Definitions and operating concepts," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 2489, no. 1, pp. 145–152, Jan. 2015.

[18] C. Wang, C. Xu, and Y. Dai, "A crash prediction method based on bivariate extreme value theory and video-based vehicle trajectory data," *Accident Anal. Prevention*, vol. 123, pp. 365–373, Feb. 2019.

[19] H. Wang, Y. Qin, W. Wang, and J. Chen, "Stability of CACC-manual heterogeneous vehicular flow with partial CACC performance degrading," *Transportmetrica B, Transp. Dyn.*, vol. 7, no. 1, pp. 788–813, Dec. 2019.

[20] Y. Guo, Z. Li, Y. Wu, and C. Xu, "Evaluating factors affecting electric bike users' registration of license plate in China using Bayesian approach," *Transp. Res. F, Traffic Psychol. Behaviour*, vol. 59, pp. 212–221, Nov. 2018.

[21] H. Liu, X. Kan, S. E. Shladover, X.-Y. Lu, and R. E. Ferlis, "Modeling impacts of cooperative adaptive cruise control on mixed traffic flow in multi-lane freeway facilities," *Transp. Res. C, Emerg. Technol.*, vol. 95, pp. 261–279, Oct. 2018.

[22] V. Milanes, S. E. Shladover, J. Spring, C. Nowakowski, H. Kawazoe, and M. Nakamura, "Cooperative adaptive cruise control in real traffic situations," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 1, pp. 296–305, Feb. 2014.

[23] Y. Guo, Z. Li, Y. Wu, and C. Xu, "Exploring unobserved heterogeneity in bicyclists' red-light running behaviors at different crossing facilities," *Accident Anal. Prevention*, vol. 115, pp. 118–127, Jun. 2018.

[24] M. Li, Z. Li, C. Xu, and T. Liu, "Short-term prediction of safety and operation impacts of lane changes in oscillations with empirical vehicle trajectories," *Accident Anal. Prevention*, vol. 135, Feb. 2020, Art. no. 105345.

[25] Chen, Song, and Ma, "Investigation on the injury severity of drivers in rear-end collisions between cars using a random parameters bivariate ordered probit model," *Int. J. Environ. Res. Public Health*, vol. 16, no. 14, p. 2632, 2019.

[26] J. H. Cheon, K. Han, S.-M. Hong, H. J. Kim, J. Kim, S. Kim, H. Seo, H. Shim, and Y. Song, "Toward a secure drone system: Flying with real-time homomorphic authenticated encryption," *IEEE Access*, vol. 6, pp. 24325–24339, 2018.

[27] C. Xu, J. Zhao, and P. Liu, "A geographically weighted regression approach to investigate the effects of traffic conditions and road characteristics on air pollutant emissions," *J. Cleaner Prod.*, vol. 239, Dec. 2019, Art. no. 118084.

[28] C. Y. Dong, H. Wang, W. Wang, Y. Li, and X. D. Hua, "Hybrid traffic flow model for intelligent vehicles exiting to off-ramp," *Acta Phys. Sinica*, vol. 67, no. 14, Jul. 2018, Art. no. 144501.

[29] F. Chen, S. Chen, and X. Ma, "Analysis of hourly crash likelihood using unbalanced panel data mixed logit model and real-time driving environmental big data," *J. Saf. Res.*, vol. 65, pp. 153–159, Jun. 2018.
[30] Y. Liu, Z. Liu, and R. Jia, "DeepPF: A deep learning based architecture for metro passenger flow prediction," *Transp. Res. C, Emerg. Technol.*, vol. 101, pp. 18–34, Apr. 2019.
[31] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017.
[32] A. Taylor, S. Leblanc, and N. Japkowicz, "Probing the limits of anomaly detectors for automobiles with a cyberattack framework," *IEEE Intell. Syst.*, vol. 33, no. 2, pp. 54–62, Mar. 2018.
[33] C. Urquhart, X. Bellekens, C. Tachtatzis, R. Atkinson, H. Hindy, and A. Seeam, "Cyber-security internals of a skoda octavia vRS: A hands on approach," *IEEE Access*, vol. 7, pp. 146057–146069, 2019.
[34] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 126–132, Jun. 2015.
[35] Z. Abdollahi Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, Dec. 2018.
[36] X. Gu, M. Abdel-Aty, Q. Xiang, Q. Cai, and J. Yuan, "Utilizing UAV video data for in-depth analysis of drivers' crash risk at interchange merging areas," *Accident Anal. Prevention*, vol. 123, pp. 159–169, Feb. 2019.
[37] Y. Pan, S. Chen, F. Qiao, S. V. Ukkusuri, and K. Tang, "Estimation of real-driving emissions for buses fueled with liquefied natural gas based on gradient boosted regression trees," *Sci. Total Environ.*, vol. 660, pp. 741–750, Apr. 2019.
[38] Y. Qin, H. Wang, and B. Ran, "Impact of connected and automated vehicles on passenger comfort of traffic flow with Vehicle-to-vehicle communications," *KSCE J. Civil Eng.*, vol. 23, no. 2, pp. 821–832, Feb. 2019.
[39] M. Wang, S. P. Hoogendoorn, W. Daamen, B. van Arem, B. Shyrokau, and R. Happee, "Delay-compensating strategy to enhance string stability of adaptive cruise controlled vehicles," *Transportmetrica B, Transp. Dyn.*, vol. 6, no. 3, pp. 211–229, Jul. 2018.
[40] P. Wang, G. Yu, X. Wu, H. Qin, and Y. Wang, "An extended car-following model to describe connected traffic dynamics under cyberattacks," *Phys. A, Stat. Mech. Appl.*, vol. 496, pp. 351–370, Apr. 2018.
[41] D.-F. Xie, X.-M. Zhao, and Z. He, "Heterogeneous traffic mixing regular and connected vehicles: Modeling and stabilization," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 6, pp. 2060–2071, Jun. 2019.
[42] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 263–284, 1st Quart., 2016.
[43] J. Reilly, S. Martin, M. Payer, and A. M. Bayen, "Creating complex congestion patterns via multi-objective optimal freeway traffic control with application to cyber-security," *Transp. Res. B, Methodol.*, vol. 91, pp. 366–382, Sep. 2016.
[44] R. E. Wilson, "Mechanisms for spatio-temporal pattern formation in highway traffic models," *Phil. Trans. Roy. Soc. A: Math., Phys. Eng. Sci.*, vol. 366, no. 1872, pp. 2017–2032, Jun. 2008.
[45] J. Santa, A. F. Gómez-Skarmeta, and M. Sánchez-Artigas, "Architecture and evaluation of a unified V2 V and V2I communication system based on cellular networks," *Comput. Commun.*, vol. 31, no. 12, pp. 2850–2861, Jul. 2008.
[46] C. Oh, S. Park, and S. G. Ritchie, "A method for identifying rear-end collision risks using inductive loop detectors," *Accident Anal. Prevention*, vol. 38, no. 2, pp. 295–301, Mar. 2006.
[47] H. Ge, R. Xia, H. Sun, Y. Yang, and M. Huang, "Construction and simulation of rear-end conflicts recognition model based on improved TTC algorithm," *IEEE Access*, vol. 7, pp. 134763–134771, 2019.
[48] M. Muzammel, M. Z. Yusoff, and F. Meriaudeau, "Event-related potential responses of motorcyclists towards rear end collision warning system," *IEEE Access*, vol. 6, pp. 31609–31620, 2018.
[49] K. Zhang, S. Batterman, and F. Dion, "Vehicle emissions in congestion: Comparison of work zone, rush hour and free-flow conditions," *Atmos. Environ.*, vol. 45, no. 11, pp. 1929–1939, Apr. 2011.