Evaluating Cybersecurity Risks of Cooperative Ramp Merging in Mixed Traffic Environments

IMAGE LICENSED BY INGRAM PUBLISHING

***Abstract*—**Connected and automated vehicle (CAV) technology has the potential to greatly improve transportation mobility, safety, and energy efficiency. However, ubiquitous vehicular connectivity also opens up the door to cyberattacks. In this study, we investigate cybersecurity risks of a representative cooperative traffic management application, i.e., highway on-ramp merging, in a mixed traffic environment. We develop threat models with two trajectory spoofing strategies on CAVs to create traffic congestion and devise an attack-resilient strategy for system defense. Furthermore, we leverage VEhicular NeTwork Open Simulator, a Veins extension simulator made for CAV applications, to evaluate cybersecurity risks of the attacks and performance of the proposed defense strategy. A comprehensive case study is conducted across different traffic congestion levels, penetration rates of CAVs, and attack ratios. As expected, the results show that mobility performance decreases up to 55.19% in the worst case when the attack ratio increases, as do safety and energy. With our proposed mitigation defense algorithm, the system's cyberattack resiliency is greatly improved.**

Digital Object Identifier 10.1109/MITS.2022.3151097
Date of current version: 5 April 2022

1939-1390/22©2022IEEE

Xuanpeng Zhao, Ahmed Abdo, and Xishun Liao
Are with the Department of Electrical and Computer Engineering, University of California, Riverside, Riverside, California, 92507, USA. E-mail: xzhao094; aabdo003; xliao016@ucr.edu

Matthew J. Barth and Guoyuan Wu
Are with the Center for Environmental Research and Technology, University of California, Riverside, Riverside, California, 92507, USA. E-mail: barth; gywu@cert.ucr.edu

Connected and Automated Vehicle Technology

The ever-increasing number of vehicles on our roads negatively impacts safety, traffic efficiency, and the environment. In terms of safety, according to data from the World Health Organization, road traffic injuries caused approximately 1.35 million deaths worldwide in 2016 [1]. Moreover, a study by the Massachusetts Institute of Technology in 2013 indicated an annual 53,000 premature deaths due to health problems caused by vehicle emissions [2]. To address these problems, connected and automated vehicle (CAV) technology has the potential to reduce traffic accidents, enhance quality of life, and improve efficiency of our transportation system [3]. CAVs can not only perceive the surrounding environment with onboard sensors such as cameras, radar, and lidar but also communicate with each other or with roadside infrastructure via vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communications. This enables CAVs and other road users to perform specific operations efficiently and collaboratively.

As a representative scenario for highway driving, ramp merging has received significant attention over the years. Various traffic control strategies have been applied at ramp merging to regulate vehicular inflow rates to avoid mainline traffic breakdowns. A widely used ramp management strategy for legacy vehicles is ramp metering, which governs on-ramp vehicles' entry to the mainline by traffic lights [4]. However, ramp metering often introduces stop-and-go maneuvers [5], [6], which significantly degrade overall system performance. To address this issue, many researchers have leveraged CAV technology and developed advanced ramp merging systems [7], which can coordinate CAVs into platoons or closely-spaced strings to maximize the throughput while smoothing speed trajectories [5], [8]. Such cooperative highway on-ramp merging systems are expected to significantly reduce traffic congestion by sharing information and implementing appropriate control measures.

It is clear that legacy vehicles and CAVs (with varying penetration rates, connectivity capabilities, and automation levels) will have to share the roads during a transition period, which may span several decades. Therefore, it is more realistic and valuable to develop an effective ramp merging strategy for mixed traffic and investigate its performance in terms of safety, efficiency, and environmental sustainability [9], [10]. Many researchers have dug into this problem with different methods [11]–[13], but they fail to address potential cybersecurity risks in communication and perception. To ensure resilient operation and the safety of all road users, potential exposure of cyberattacks [14] should be considered for real-world implementation, and a cybersecurity-awareness defense strategy should be carefully designed.

This article reveals the potential cybersecurity risk of a highway ramp merging strategy under mixed traffic and provides an effective defense solution. More specifically, the three major contributions of this article are as follows:

1) Two spoofing strategies are designed, which cannot be detected through inconsistent speed and position information, for the cooperative highway on-ramp merging strategy
2) A minimum mean-square estimation (MMSE)-based defense algorithm is devised to detect the attacks and mitigate their negative impacts on the entire traffic.
3) A comprehensive evaluation is conducted for the cybersecurity risks of the proposed merging strategy with these two attacks and the performance of the corresponding defense strategy.

Background

In this section, we briefly review relevant studies on CAV-based cooperative highway on-ramp merging applications and potential cybersecurity risks in CAV applications. We also introduce a simulation environment for analyzing traffic impacts of cyberattacks.

CAV-Based Cooperative Ramp Merging

The authors of [5] proposed a cooperative merging system based on V2X communications and adopted a microscopic traffic simulator to evaluate its performance in terms of highway capacity. The basic idea is to use roadside unit (RSU)-equipped infrastructure to collect onboard

As a representative scenario for highway driving, ramp merging has received significant attention over the years.

unit-equipped vehicles' information in the form of basic safety messages (BSMs) [15] via V2V and V2I communications. With this information, the system can provide speed guidance to the involved CAVs to improve merging efficiency. Zhao et al. [8] developed a hierarchical CAV-based ramp management system that can perform cooperative merging maneuvers for CAVs at the individual ramp level and simultaneously regulate the inflow rates of multiple ramps. Some of these existing studies assume a full penetration rate of CAVs for effective ramp merging control. The feasibility and performance of their algorithms in mixed traffic still need to be verified. Chen et al. [16] offered a hierarchical control approach consisting of both a tactical and operational layer to enable efficient and safe merging operations. Rios-Torres and Malikopoulos [17] put forward a coordination strategy that allows vehicles to merge without creating congestions under collision-avoidance constraints, thus reducing both fuel consumption and travel time. Davis [9] showed that traffic congestion might be significantly mitigated even with a 50% penetration rate of adaptive cruise control-enabled vehicles. It is noted that most of these ramp merging-related studies for mixed traffic do not consider potential cybersecurity issues.

Cybersecurity for CAV-Based Applications

Bhat [18] presented an overview of commonly seen security risks associated with both automotive radar and dedicated short-range communication (DSRC) systems, such as jamming and spoofing. According to the authors of [19], jamming attacks include denial-of-service (DOS) and distributed DOS (DDOS) attacks, while spoofing attacks comprise black-hole, Sybil, and replay kinds. In this article, we focus on man-in-the-middle attacks. Chen et al. [20] investigated cybersecurity vulnerabilities in the intelligent traffic signal system (I-SIG) application and concluded that current signal control algorithms are highly vulnerable to data spoofing attacks, even only one single attacked vehicle. They also assumed that I-SIG [21] had utilized the Security and Credential Management System (SCMS) [22]. This required every BSM to be signed by the sender's digital certificate to ensure the message's integrity before CAVs and infrastructure were allowed to participate in further communications. Thus, the receiver could verify the sender's identity by the signature. This study also assumes that the SCMS has been deployed to ensure that all the BSMs are authenticated. Cui et al. [23] developed an evaluation platform that simulated vehicles' sensor errors and communication delays to investigate the effect of cyberattacks on the cooperative adaptive cruise control. They deployed heuristic cyberattacks on the third vehicle in the platoon by assigning constant errors on the GPS and radar information since the preset time step. Such attacks can be easily detected due to large position jumps, lane overtaking, and inconsistent speeds/positions. In this article, we propose two attack strategies that are hard to be detected by checking for data inconsistency.

Wang et al. [24] incorporated the intelligent driver model and communication scheme to numerically analyze cyberattack effects on connected automated vehicular platoons without a comprehensive evaluation in a microscopic simulation environment. In [25], the authors deployed three different attack methods on the proposed collective perception-based on-ramp merging control algorithm and measured their impacts. However, they did not provide an effective defense method to mitigate the potential attacks. Xu et al. [26] focused on the sensor perception aspect and aimed to reveal the security risks of onboard sensors. They proposed two defense strategies against their well-designed attacks on ultrasonic sensors to improve system resilience and validated them in both simulation and the real world. Giraldo and Cardenas [27] proposed a moving-target defense strategy for multivehicle systems to mitigate the impacts caused by cyberattacks. Liu et al. [28] presented an attack-resistant location-estimation approach based on the MSE of distance difference between the declared distance and the distance determined by the received signal strength index (RSSI) [29] of the radio signal to tolerate malicious attacks. The RSSI is an indicator of signal quality and widely used to calculate received signal power [30]. In wireless channel models, received power is inversely proportional to the distance between the sender and receiver. Motivated by this idea, in this study, we develop a secure and resilient defense strategy to detect and filter out malicious attacks. Although RSSI localization has relatively lower accuracy than other ranging techniques due to multipath radio signals' propagation [31], it is considered a cost-effective method for rough position estimation [32], [33] and is suitable for our study purposes.

Simulation Environment

In this study, we adopt and utilize VEhicular NeTwork Open Simulator (VENTOS) [34] to perform the simulation. VENTOS is a Veins extension simulator for modeling vehicular traffic flows, collaborative driving, and interactions among or between CAVs and infrastructure equipped with DSRC. DSRC [35] is a wireless communications standard featuring reliable and low-latency data transmission. More

specifically, VENTOS combines the capabilities of both vehicular traffic simulation from Simulation of Urban Mobility (SUMO) [36] and communication network simulation from Objective Modular Network Testbed in C++ (OMNET++) [37]. SUMO is a highly portable, microscopic, and continuous traffic simulator designed to handle large roadway networks, while OMNET++ is a C++ simulation library that can simulate high-fidelity, complex communication networks.

> The LC2013 lane-changing model was developed by Jakob Erdmann and consists of four different motivations for lane changes: strategic, cooperative, tactical, and regulatory.

Methodology

In this section, we present the mixed traffic cooperative highway on-ramp merging algorithm to be used in the simulation, followed by an elaborate description of threat models and defense strategies. The general assumptions in this study are as follows:

- All CAVs consistently send BSMs, including positions, speeds, and accelerations, via V2I communications to the RSU-equipped infrastructure. Furthermore, they strictly follow the speed guidance recommended by the infrastructure.
- In the network with a multilane mainline segment, only CAVs involved in merging maneuvers (i.e., those vehicles on the merging lanes) would be controlled by the proposed algorithm and are susceptible to attacks by the malicious actor.
- We assume that the attacker can only modify the content of BSMs but not manipulate the radio signal strength within the effective area, which is defined as the *overlapped region of both the RSU's and the attacker's communication coverage* (given that the RSU is within the attacker's coverage).
- We also assume that the SCMS is deployed and cannot be exploited, which means that the attacker cannot falsify the signatures of senders.

Cooperative Highway On-Ramp Merging Algorithm in Mixed Traffic

The proposed cooperative highway on-ramp merging system relies on V2I communications. When CAVs on the on-ramp and rightmost lane of the mainline enter the communication range of the RSU-equipped infrastructure in the merging area, they broadcast their state information via BSMs. After receiving the involved CAVs' states, the RSU will perform the proposed ramp merging algorithm (shown in Figure 2) to determine the merging sequence and longitudinal speed for each CAV and broadcast this information to enable cooperative maneuvers. The overall system architecture is illustrated in Figure 1. First, we specify upstream roadway

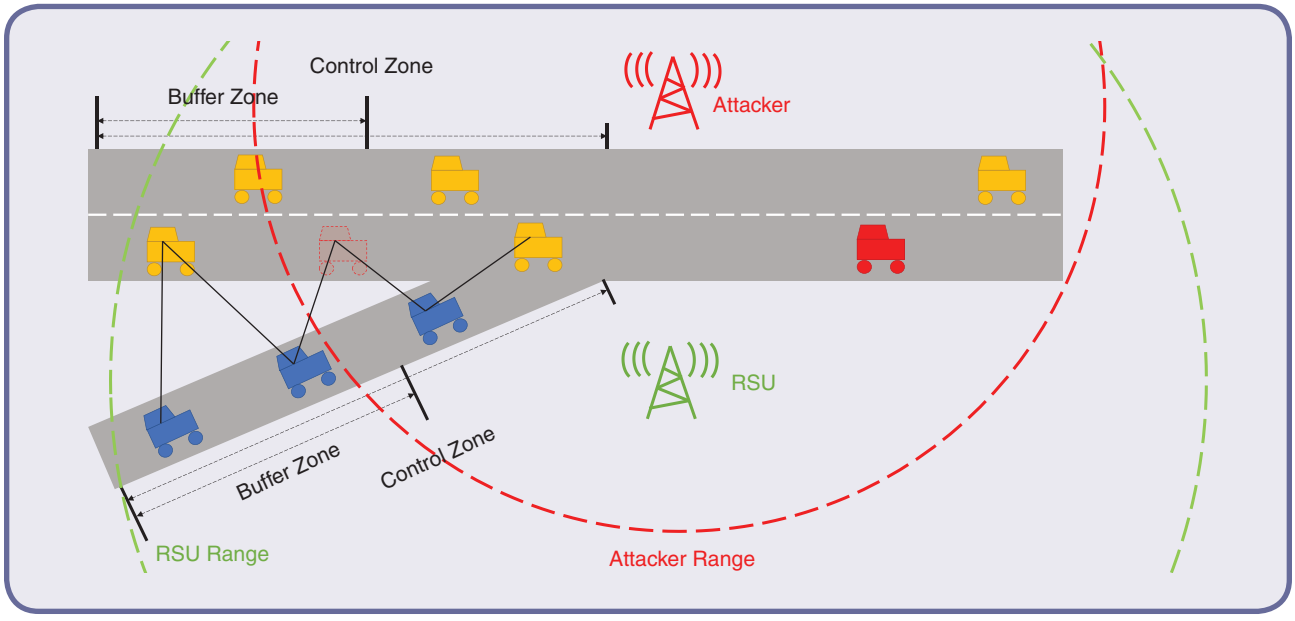


FIG 1 The overall system architecture of the threat models.

When traffic is light, benefits from the increasing penetration rate of CAVs could not offset the negative impacts due to cyberattacks.

segments with respect to the merging area (within the RSU communication range) with two types of zones: control and buffer zones. In buffer zones, the RSU can sort out the incoming CAVs based on their distances to the merging point. In control zones, the RSU sends recommended speeds back to respective CAVs. The flowchart of the system is shown in Figure 2.

Vehicle Sequence Algorithm

The RSU collects the information from CAVs on both the mainline and on-ramp via V2I communications and determines their entrance sequence based on their distances to the merging point. Moreover, if the distance between two CAVs is too far (e.g., due to legacy vehicles), we split the string into two and create a new leader for the new string. We then apply customized motion control for each string of CAVs.

Motion Control Algorithm

Once CAVs are arranged into strings, the RSU will apply the following control algorithm to enable cooperatively merging maneuvers. The control algorithm can compute the recommended speed for every following vehicle based on the state of its predecessor. Li et al. [38] provided a general car-following model that can be used to describe vehicles' longitudinal dynamics:

$$\dot{x}_n(t) = v_n(t) \tag{1}$$

$$\dot{v}_n(t) = f(s_{n(t)}, v_n(t), \Delta v_n(t)). \tag{2}$$

Based on this model, we conduct our control algorithm for acceleration of the ego vehicle:

$$\begin{aligned} a(t) = {} & k_d * (S_{\text{headway}}(t) - S_{\text{length}}(t) - S_{\text{safe gap}}(t)) \\ & + (v_{\text{front}}(t) - v_{\text{self}}(t)) * k_v, \end{aligned} \tag{3}$$

where $a(t)$ is acceleration of the ego vehicle at time step t; k_d and k_v are control gains for distance and speed, respectively; S_{headway} is the distance between the ego vehicle and its predecessor; S_{length} is the ego vehicle's length; $S_{\text{safe gap}}$ is the safety distance gap, which can guarantee minimum clearance between two vehicles; $v_{\text{front}}(t)$ is the velocity of the front vehicle at time step t; and $v_{\text{self}}(t)$ is the velocity of the ego vehicle at time step t.

Thus, the recommended speed can be derived based on the acceleration.

$$v(t) = a(t) * t_{\text{step}} + v_{\text{self}}(t-1), \tag{4}$$

where t_{step} is the simulation time step, and $v_{\text{self}}(t-1)$ is the velocity of the ego vehicle at time step $(t-1)$. The leader of each string is recommended to travel at the roadway speed limit. Based on our assumptions, CAVs that are not on the rightmost lane of the mainline are not controlled by the merging algorithm. Similar to all legacy vehicles, their longitudinal behaviors are controlled by the Krauß car-following model [39], [40], and their lateral maneuvers are governed by the LC2013 lane-changing model [41].

The Krauß model is defined as [40]

$$v_{\text{safe}}(t) = v_l(t) + \frac{g(t) - g_{\text{des}}(t)}{\tau + \tau_b}, \tag{5}$$

$$v_{\text{des}}(t) = \min[v_{\max, v(t)+a(v)\Delta t, v_{\text{safe}}(t)}], \tag{6}$$

$$v(t+\Delta t) = \max[0, v_{\text{des}}(t) - \eta], \tag{7}$$

$$x(t+\Delta t) = x(t) + v\Delta t, \tag{8}$$

where g_{des} is the desired gap, τ is the reaction time of drivers, τ_b is the time for deceleration, v_{safe} is the safe speed, v_{des} is the desired speed, $v_{\max}$ is the maximum speed, and η is the random perturbation. The two major modifications on this model made by SUMO are 1) using

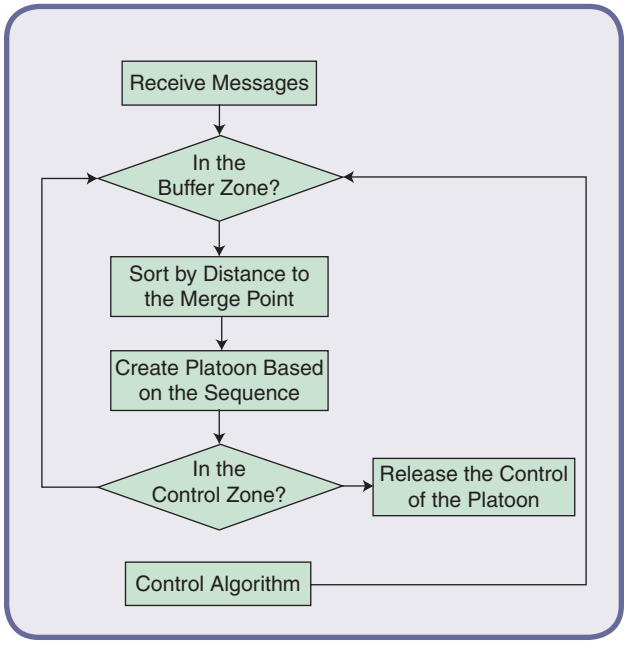


FIG 2 The system workflow of the cooperative ramp merging strategy for CAVs.

the Euler-position update rule to make the safe-speed formula suitable for maintaining safety and 2) using different deceleration capabilities to avoid violating safety [41].

The LC2013 lane-changing model was developed by Jakob Erdmann and consists of four different motivations for lane changes [41]: strategic, cooperative, tactical, and regulatory. When a vehicle (either legacy or CAV) reaches the merging point, the lane-changing model will allow the vehicle to merge when it is safe. Otherwise, the vehicle will wait for a suitable gap to merge.

To avoid the collision of a CAV with its preceding legacy vehicle in the mixed traffic simulation, we apply a heuristic gatekeeping logic by consistently comparing the recommended speed with the safe speed from the Krauß model and choosing the lower one as the target speed, i.e.,

$$v_{\text{target}} = \begin{cases} v_{\text{safe}}, & v_{\text{safe}} < v_{\text{recommended}} \\ v_{\text{recommended}}, & v_{\text{safe}} > v_{\text{recommended}} \end{cases}. \quad (9)$$

Please note that model predictive control could also be an alternative to handle this type of safety constraint [16].

Threat Models

The proposed attack strategies aim at creating congestion while not being easily detected by simple defense approaches, such as inconsistency of a vehicle's location and speed, teleporting, or same-lane overtaking. Before the elaboration of attack strategies, we illustrate the scenario setup, as presented in Figure 1. The attacker is located near the RSU and can intercept the BSMs broadcasted by equipped vehicles. Then, the attacker deploys man-in-the-middle attacks to modify the BSMs and resends them to the RSU. For example, the red vehicle is the attacked vehicle, and the dashed line represents the associated location where the attacker tries to spoof the RSU. In the following, we detail two nontrivial spoofing strategies.

Emergency Stop Spoofing

When a target CAV enters the attacker's communication range, the attacker can consistently receive BSMs from this CAV. The attacker deploys man-in-the-middle attacks, which make the CAV's location information frozen at the respective entrance point, falsify its speed information to be zero, and then resend all this information to the RSU. In this case, the control algorithm will provide incorrect, recommended speed information to those following CAVs within the same attacked vehicle string to make them slow down or even completely stop. The pseudocode is shown in Algorithm 1.

Accumulative Position Drift Spoofing

In this type of attack, the attacker keeps receiving BSMs from the target CAV after entering the attacker's communication range. Then, the attacker continuously generates falsified speed information over time, i.e., a speed profile that is slightly lower than the actual speed profile of the attacked vehicle. In addition, the spoofed location is computed based on the falsified speed, i.e.,

$$\text{speed} = \text{speed} + \text{acceleration} * \text{delta}T \quad (10)$$

$$\text{location} = \text{location} + \text{speed} * \text{delta}T + \frac{1}{2} * \text{acceleration} * \text{delta}T. \quad (11)$$

This slight inconsistency of location and speed may be considered a result of signal loss or GPS errors. However, as position drift accumulates, more severe impacts

Algorithm 1. Emergency Stop Spoofing Algorithm.

```
INPUT: BSM from target CAVs.
INITIALIZE SpFlag = 0, SpLoc, SpBSM, ActLoc, SpSpeed
IF Received a BSM from a target CAV THEN
    SpBSM = BSM
    IF SpFlag = 0 THEN
        ActLoc = location contained in the BSM
            SpLoc = ActLoc
            SpFlag = 1
    END IF
    SpSpeed = 0
    Set SpSpeed to be the speed in SpBSM
    Set SpLoc to be the location in SpBSM
    Resend the SpBSM to the RSU
END IF
```

SpFlag: Spoofing_flag; SpLoc: Spoofing_Location; SpBSM: Spoofing_BSM; ActLoc: Actual_Location; SpSpeed: Spoofing_Speed.

Algorithm 2. Accumulative Position Drift Spoofing Algorithm.

```
INPUT: BSM from target CAVs.
INITIALIZE SpFlag = 0, SpLoc, SpSpeed, LastTS, Acc = -2.5
IF Received a BSM from a target CAV THEN
    SpBSM = BSM
    IF spFlag = 0 THEN
        LastTS = time stamp contained in the BSM
        ActLoc = location contained in the BSM
            ActSpeed = speed contained in the BSM
            SpLoc = ActLoc
            SpSpeed = ActSpeed
            SpFlag = 1
    ELSEIF SpSpeed > 0 THEN
        ActTS = time stamp contained in the BSM
        DelT = LastTS - ActTS
        Compute SpSpeed using equation (10)
        Compute SpLoc using equation (11)
        LastTS = ActTS
    END IF
    Set SpSpeed to be the speed in SpBSM
    Set SpLoc to be the location in SpBSM
    Resend the SpBSM to the RSU
END IF
```

Algorithm 3. An MSE-Based Attack-Resilient Defense Algorithm.

```
INPUT: A set of BSMs from CAVs: Platoon
OUTPUT: Platoon
INITIALIZE: Flag = True, M = size of Platoon, Threshold, MMSE
WHILE M > 1 AND Flag = True
    SUM_MSE = 0
    FOR i = 0 to M
        Compute the MSE using to equation (12)
        SUM_MSE = SUM_MSE + MSE
    END FOR
    IF SUM_MSE < Threshold THEN
        BREAK
    ELSE
        SUM_MSE = 0
        FOR j = 0 to M
            FOR i = 0 to M
                IF j! = i THEN
                    Dist, Loc ← BSM of Platoon[i]
                    Compute the MSE using to equation (12)
                    SUM_MSE = SUM_MSE + MSE
                END IF
            END FOR
            IF SUM_MSE < Threshold THEN
                Flag = False
                Remove Platoon[j] from Platoon
                BREAK
            ELSEIF SUM_MSE < MMSE
                MMSE = SUM_MSE
                Delete_Vehicle = Platoon[j]
            END IF
        END FOR
        Remove Delete_Vehicle from Platoon
        M = M – 1
    END IF
END WHILE
```

(e.g., congestion) on the upstream traffic would begin to show up. The pseudocode is shown in Algorithm 2.

Defense Strategy

Motivated by Liu et al. [28], we define an MSE-based attack-resilient defense strategy to detect and filter BSMs with spoofed data on the RSU side. We exploit the advantage that once the RSU receives a BSM, the infrastructure can get the BSM's RSSI. The RSSI is approximately inversely proportional to the distance between the sender and the receiver. Our defense strategy aims to find the outlier(s) with more significant error(s) compared to others. Therefore, it does not require accurate transmission distances that would be challenging for RSSI-based estimation. In this case, the RSU receives BSMs from both CAVs and the attacker and feeds them into the vehicle sequence algorithm to identify strings. For each string, we compute MSEs of distance measurements based on the RSSI statistics and location information embedded in the received BSMs. Thus,

$$s^2 = \frac{\sum (\delta_i - \sqrt{(x_i - x)^2 + (y_i - y)^2})^2}{m}, \tag{12}$$

where δ_i is the distance measured by the RSSI for the ith CAV; x_i and y_i represent the latitude and longitude, respectively, contained in the BSM of the ith CAV; x and y are the GPS coordinates of the RSU; and m is the total number of CAVs in this string. We then define a threshold τ by the average MSE when there are no attacks:

$$\frac{\sum s_j^2}{n} < \tau^2, \tag{13}$$

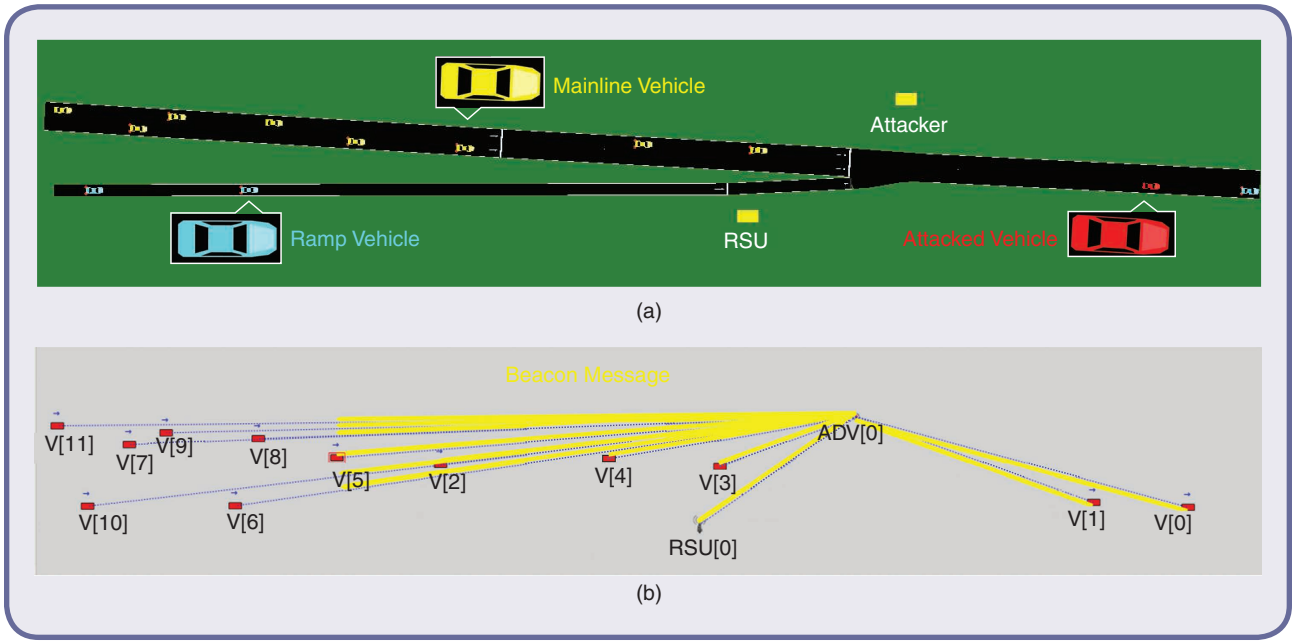


FIG 3 VENTOS simulation network and visualization. (a) A simulation network of the highway and the ramp and (b) BSM transmission visualization. ADV: adversary; V: vehicle.

where ς_j^2 is the MSE of string j that all CAVs are benign and n is the number of strings. If the MSE is lower than τ, the string is considered a benign set that does not include attacked vehicle(s). Therefore, our goal is to identify the largest benign set of CAVs' distance.

To reduce computational loads of the defense strategy, we propose a step-wise deletion greedy algorithm (as shown in Algorithm 3). This greedy algorithm starts with the initial location set, including all CAVs of the string. In subsequent time steps, the algorithm will keep verifying whether the MSE of the current set of CAVs' locations is lower than the threshold. If the answer is yes, the set is confirmed for further control. Otherwise, the algorithm computes the MSEs of all possible sets and chooses the subset with the least MSE as the input to the next time step. This algorithm continues until it finds the set that meets the threshold condition.

Simulation Study and Results

In this section, we describe the simulation's settings and parameters, evaluate the system performance, including mobility, safety, and environment under different scenarios (e.g., with and without cyberattacks as well as the defense strategy), and analyze the simulation results. We choose one traffic demand as our benchmark and evaluate the improvement or deterioration compared to the baseline (no CAVs and thus no cyberattacks).

We set up the simulation environment with VENTOS, using the network shown in Figure 3(a). The only transmission noise is "thermal noise," which is set to be –90 dBm. To make the simulation more realistic, we add noise to the vehicles' positions in the simulation based on a random walk model. A transmission power of 20 mW and data rate of 6 Mbps are chosen as the default values in VENTOS. There are two lanes on the highway segment and one on the on-ramp. Only the CAVs on the rightmost lane of the highway and the on-ramp (i.e., involved in merging maneuvers) would play a major role in this simulation controlled by the merging algorithm. With VENTOS, we can also visualize BSM transmission, as depicted in Figure 3(b). As mentioned previously, we assume that the RSSI cannot be compromised. The vehicles on the highway can change their lane freely based on the default lane-changing algorithm in SUMO. The attacks start only when the target CAV enters the attacker's effective area and stop when it exits the area. For those CAVs traveling along the mainline, we assume that attacks can be deployed immediately once the target CAVs are traveling on the rightmost lane and continuously take effect even when they change to the left lane afterward, as long as they are still within the attacker's range. In the simulation study, we set the traffic demand ratio between highway and on-ramp to 3:1, and the roadway capacity to be 2,000 passenger car units per hour per lane (pcu/h/ln). With different volume-to-capacity (V2C)

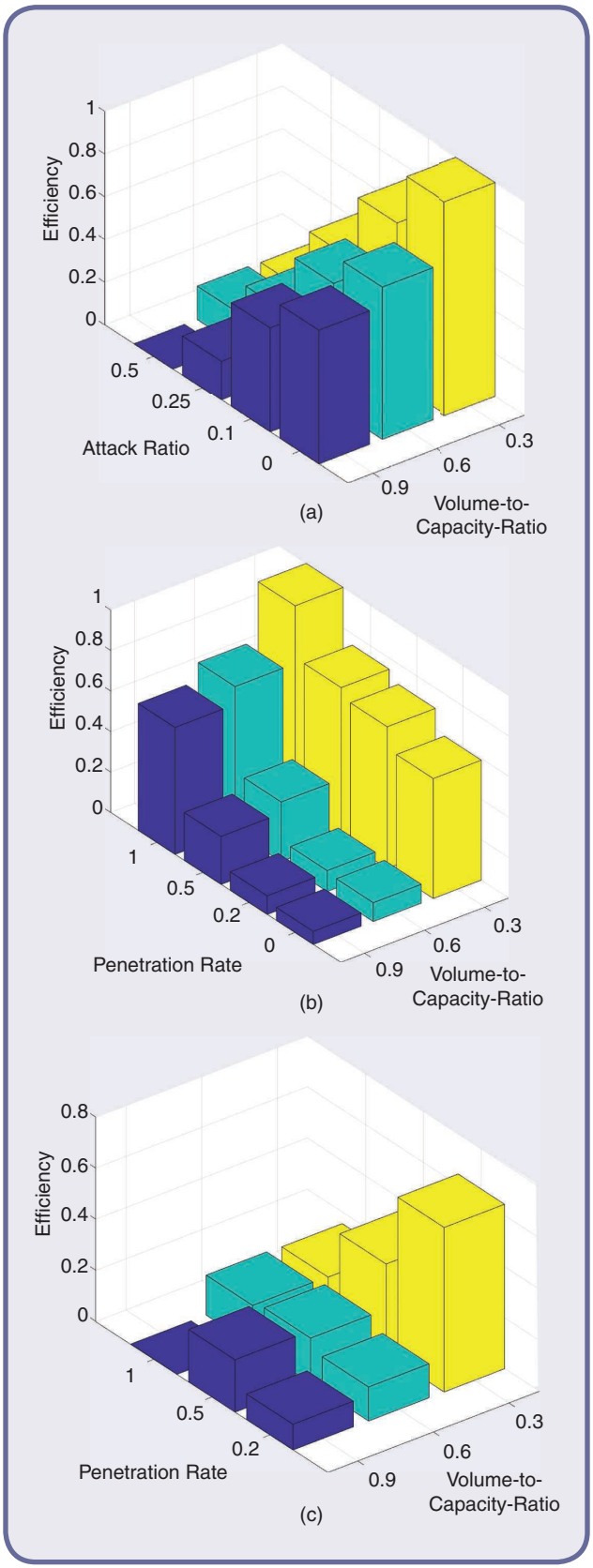


FIG 4 The bar charts of efficiencies in different cases. (a) A 100% penetration rate, (b) zero attack ratio, and (c) 0.5 attack ratio.

Table 1. The traffic flow mobility performance of selected simulation cases.

Case Index	Penetration Rate	Attack Ratio	V2C Ratio	VMT (mi)	VHT (h)	Efficiency (mi/h)
1	100	0.5	0.9	26	2.4	10.9
2	50	0.5	0.9	68.7	4.5	15.4
3	20	0.5	0.9	89.1	6.8	13.1
4	100	0.25	0.9	38.9	2.6	14.9
5	50	0.25	0.9	68.8	4.5	15.2
6	20	0.25	0.9	90.9	7.2	12.7
10	100	0	0.9	97.7	4	24.4
27	100	0.5	0.3	31.2	2.2	14.2
28	50	0.5	0.3	60.2	3.3	18.5
29	20	0.5	0.3	70.7	2.9	24.8
31	50	0.25	0.3	63.2	2.9	22.1
34	50	0.1	0.3	64.1	2.7	23.5
37	50	0	0.3	67	2.5	26.9

Table 2. The traffic flow safety performance of selected simulation cases.

Case Index	Penetration Rate (%)	Attack Ratio	V2C Ratio	Velocity Mean Absolute Deviation (m/s)	Velocity Standard Deviation (m/s)	Acceleration Mean Absolute Deviation (m/s^2)	Acceleration Standard Deviation (m/s^2)
28	50	0.5	0.3	5.81	5.14	3.05	3.76
31	50	0.25	0.3	5.15	3.96	3.47	4.07
33	100	0.1	0.3	5.86	4.37	2.98	3.82
34	50	0.1	0.3	2.98	2.56	3.53	4.12
35	20	0.1	0.3	2.68	1.84	4	4.46
36	100	0	0.3	2.19	1.05	2.89	3.72
37	50	0	0.3	2.38	1.38	3.78	4.3
38	20	0	0.3	2.69	1.46	3.99	4.45
39	0	0	0.3	2.96	1.93	4.05	4.47

Table 3. The traffic flow energy performance of selected simulation cases.

Case Index	Penetration Rate (%)	Attack Ratio	V2C Ratio	Fuel (gal/mi)	CO (gal/mi)	HC (gal/mi)	NOx (gal/mi)	PM 2.5 (gal/mi)	CO_2 (gal/mi)
28	50	0.5	0.3	187.6	1.6515	0.0137	0.0729	0.0036	598.9
31	50	0.25	0.3	178.3	1.6376	0.0134	0.0712	0.0034	569.5
34	50	0.1	0.3	173.3	1.7115	0.0137	0.07	0.0035	553.5
37	50	0	0.3	166	1.5427	0.0126	0.0672	0.0032	530.2

CO: carbon monoxide; HC: hydrocarbon; NOx: nitrogen oxide; PM: particulate matter.

ratios, we schedule each vehicle's departure time using a Poisson distribution.

We evaluate the performance of mobility with four CAV penetration rates (i.e., 0, 20, 50, and 100%), three V2C ratios (i.e., 0.3, 0.6, and 0.9), and four attack ratios (i.e., 0, 0.1, 0.25, and 0.5), which represent the percentages of attacked CAVs with respect to the entire CAV population. As evaluating a nonzero attack ratio in a non-CAV scenario is meaningless, we focus on 39 different cases in total. The simulation time for each run is set to 20 min. The mobility performance is measured by the network efficiency,

$$Q = \frac{VMT}{VHT}, \tag{14}$$

where VMT and VHT are the total vehicle miles traveled and total vehicle hours traveled in the network, respectively. The efficiencies of three typical cases are presented in Figure 4. Figure 4(a) shows the efficiency as a mapping of both attack and V2C ratios under a 100% CAV penetration rate. It can be observed that efficiencies decrease as the attack ratio increases. From Figure 4(a) and (b), it can be seen that as the V2C ratio decreases, efficiencies increase. In the case without an attack, we note the positive correlation between penetration rate and efficiency. By observing Figure 4(c), where the attack ratio is 0.5, we note that the results are quite different from Figure 4(b). Because of the attack, the system performance would vary under different V2C ratios. When traffic is light, benefits from the increasing penetration rate of CAVs could not offset the negative impacts due to cyberattacks. Therefore, the system efficiency decreases as the penetration rate increases. When traffic gets more congested, system efficiency may peak at the penetration rate level of 50%.

Table 1 summarizes the overall mobility performance of selected cases. As expected, higher penetration rates mean higher mobility efficiencies in a nonattack scenario with a fixed V2C ratio. However, this observation does not hold under attacks. As shown in cases 27, 28, and 29 (i.e., with a 0.5 attack ratio), efficiencies decrease significantly with increasing CAV penetration rates. When the attack ratio is 0.25 (e.g., cases 4, 5, and 6), the difference in efficiency is not significant, but VMT drops rapidly when the penetration

rate increases. This indicates that traffic gets more congested, and spawning of vehicles in simulation is even blocked. Under the same penetration rate, as the V2C ratio is reduced, deploying more attacks can reduce efficiency (see cases 28, 31, 34, and 37). With the same attack ratio (e.g., 0.25 or 0.5) and a high V2C ratio (e.g., 0.9), efficiencies show slight fluctuations, as indicated in cases 1, 2, 3, and 4. One hypothesis is that vehicles are moving slowly on

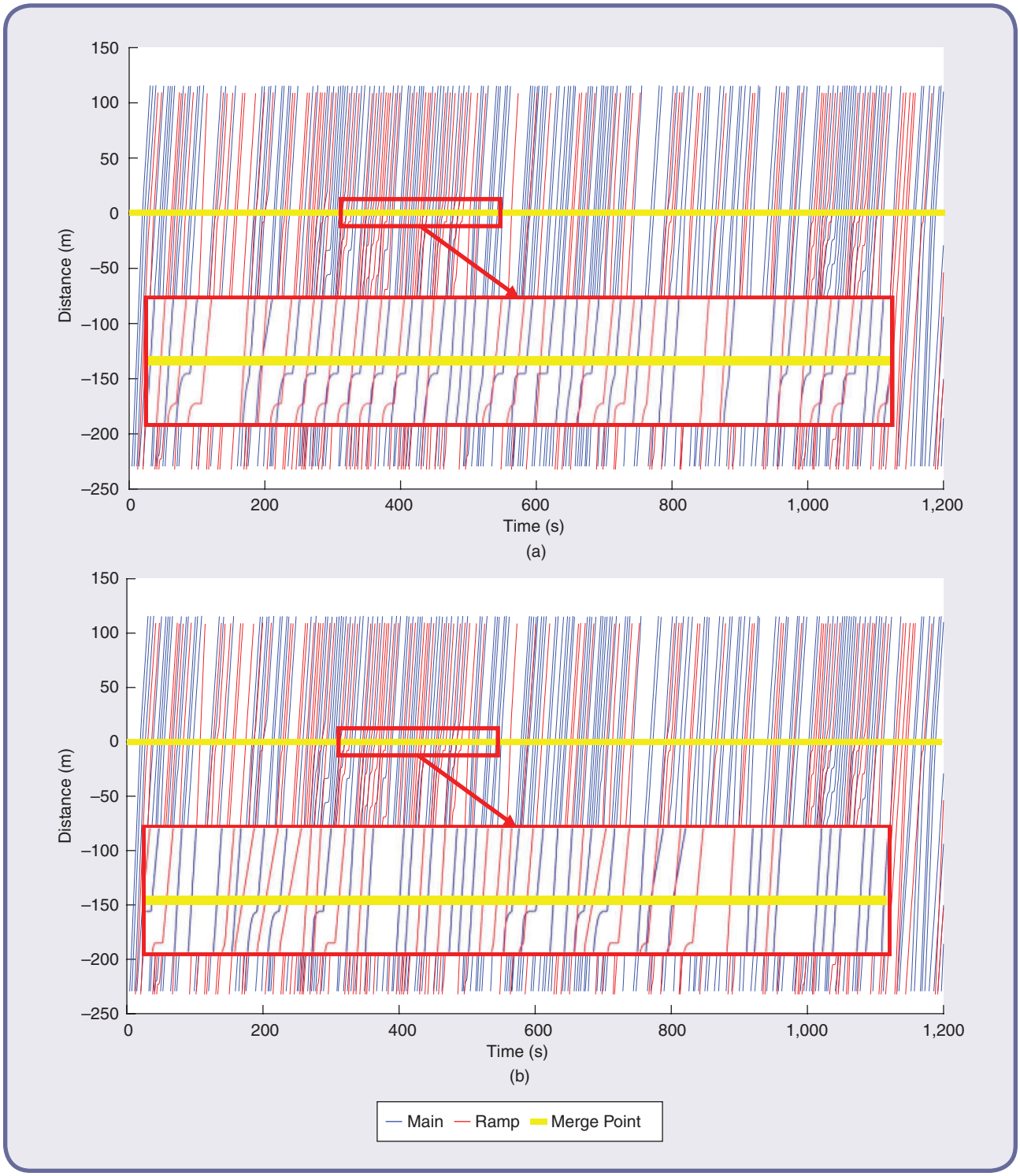


FIG 5 The time-space diagrams of two cases with different penetration rates, with a zero attack ratio and a 30% volume-to-capacity ratio. (a) The baseline and (b) a 50% penetration rate.

the entire approach when the traffic volume reaches the road capacity. In these cases, increasing the attack ratio introduces more chaos into the network, reducing traffic throughput at the bottleneck (i.e., the ramp merging area), as observed from the VMT values. In particular, the most congested case is case 1, whose efficiency is only 10.9 mi/h, 55.19% worse than its counterpart—case 10 (with the same V2C ratio and penetration rate but no attacks).

On the other hand, we quantify the safety risks due to cyberattacks in terms of driving volatility, representing vehicle movement stability. In this article, standard deviation and mean absolute deviation measurements [42] are used for computing driving volatility, which are defined, respectively, as

$$S_{\text{dev}} = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{x})^2} \tag{15}$$

$$D_{\text{mean}} = \frac{1}{n}\sum_{i=1}^{n}|x_i - \bar{x}|, \tag{16}$$

where n is the total number of observations, x_i represents the ith of observations, $\bar{x}$ is the mean of observations, and S_{dev} is the standard deviation. A larger deviation means higher driving volatility.

As listed in Table 2, deviations of velocity and acceleration decrease when penetration rates rise under the scenarios of nonattack and fixed traffic volumes. In particular, when the penetration rate is 50% (i.e., cases 28, 31, 34, and 37), the deviation of acceleration reduces while the deviation of velocity increases, as the attack ratio grows. Please note that high velocity deviation means instability in traffic.

We further analyze energy consumption and pollutant emissions with the U.S. Environmental Protection Agency's MOtor Vehicle Emission Simulator (MOVES) [43]. The selected results are summarized in Table 3. From this table, it can be observed that with increase of the CAV penetration rate, fuel consumption and carbon dioxide (CO_2) emissions decrease, which matches the conclusion by Wang et al. [5]. According to cases 28, 31, 34, and 37, we can conclude that fuel consumption and CO_2 and nitric oxide emissions are positively correlated with the attack ratio.

To investigate system performance under the other attack strategy and defense algorithm, we select the benchmark scenario with 900 pcu/h/ln on the highway and 300 pcu/h/ln on the on-ramp under a 0.3 V2C ratio. The baseline case is set with the same demand: a 0% penetration rate and zero attack ratio, whose time-space diagram is shown in Figure 5(a). The total VMT and VHT of the baseline case are 67.1 mi and 2.8 h, respectively, and the network efficiency is 23.7 mi/h. Figure 5(b) presents the time-space diagram for the scenario, with a 50% CAV

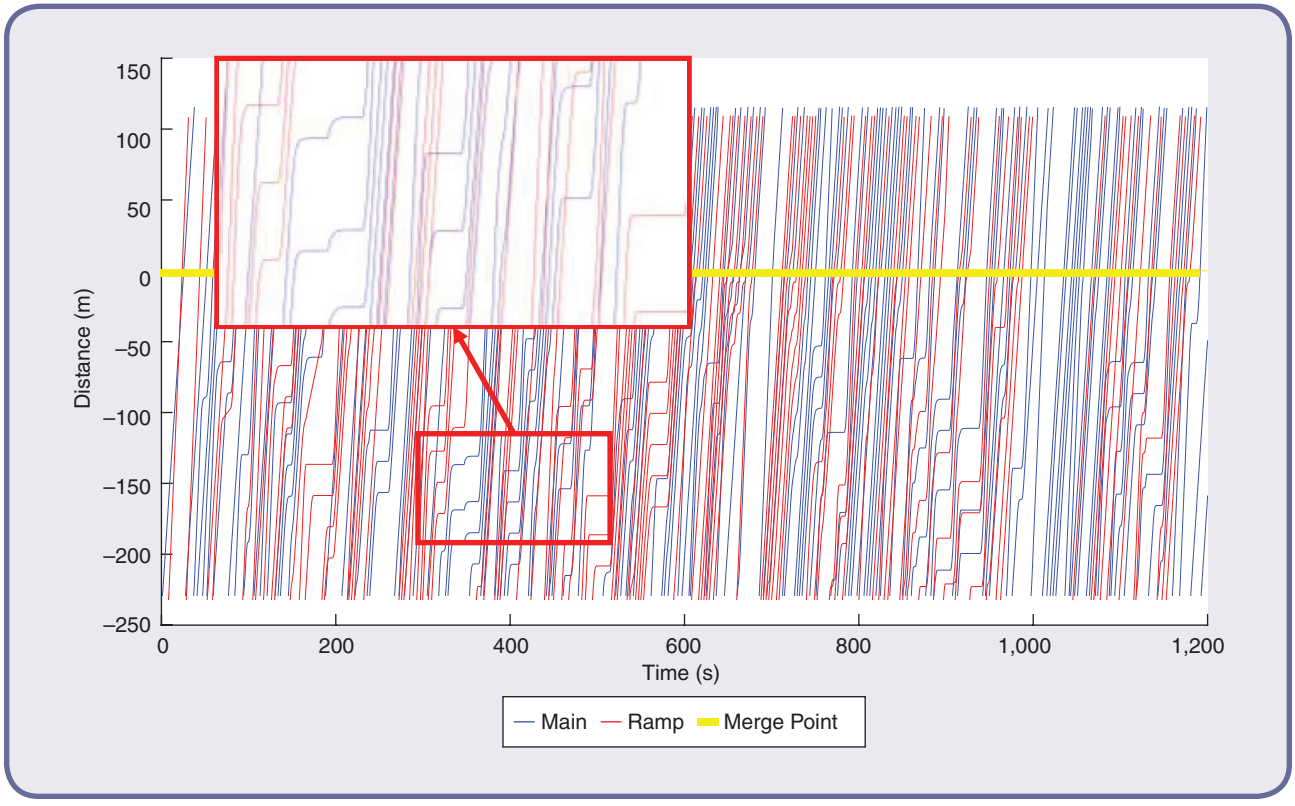


FIG 6 Time-space diagrams under accumulative position drift spoofing attacks with a 0.5 attack ratio.

penetration rate. Compared to the baseline, network efficiency increases by 13.9% (to 26.9 mi/h). As displayed in the zoom-in parts of the time-space diagrams at the ramp merging area, applying the proposed merging strategy can significantly help mitigate upstream shockwaves and smooth vehicle trajectories.

> Note that it is not necessary to base our proposed attack and defense strategies on DSRC, but they applicable to other communication technologies, including cellular V2X.

Next we enable the attacker's behaviors with a 0.5 attack ratio. Under the first attack strategy, VMT is decreased to 60.2 mi, VHT is reduced to 3.3 h, and the network efficiency is only 18.5 mi/h. With the same attack ratio, we deploy the second attack strategy, i.e., accumulative position drift spoofing, and traffic gets more congested. The efficiency is 17.9 mi/h, and VMT and VHT are 48.6 mi and 2.7 h, respectively. The time-space diagram of the second attack strategy is illustrated in Figure 6. It can be observed from the zoom-in area in Figure 6 that the shockwaves created by attacks occur much more frequently and last much longer compared to the case without attacks. We also deploy the proposed defense algorithm to detect and filter out the malicious information created by attacks. Due to introduction of the defense algorithm, the network efficiencies under the first and second attack strategies become 26.2 and 25 mi/h, respectively, both of which are much better than the associated cases without defense and nearly as close to the cases without attacks. Figure 7 depicts the time-space diagram after implementing the defense strategy under the second attack strategy. As represented by the smoother trajectories and fewer shockwaves in the figure, the defense strategy can help alleviate the congestion caused by attacks. Table 4 summarizes key statistics of representative scenarios.

Conclusions and Future Work

This study revealed the cybersecurity risks of a typical CAV application, i.e., cooperative highway on-ramp merging in a mixed traffic environment. Two nontrivial cyberattack strategies, i.e., emergency stop spoofing and accumulative position drift spoofing, were proposed and

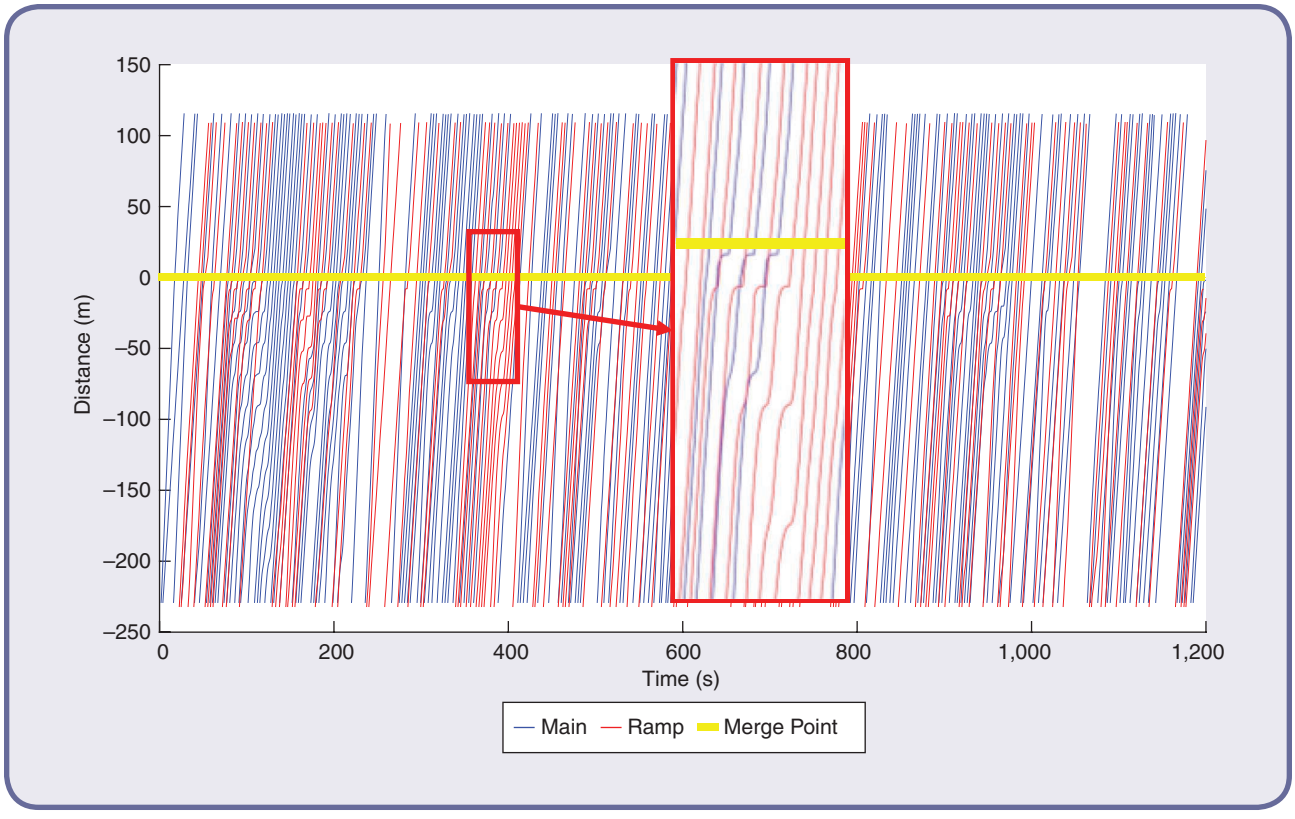


FIG 7 Time-space diagrams under the second type of attacks with a defense strategy.

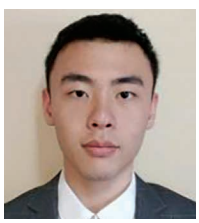
Table 4. The traffic flow mobility performance of each simulation case.

	VMT (mi)	VHT (h)	Efficiency (mi/h)
Baseline (0% penetration rate, zero attack ratio, 30% V2C ratio)	67.1	2.8	23.7
Cooperative merging system (50% penetration rate)	67	2.5	26.9
Emergency stop spoofing (0.5 attack ratio)	60.2	3.3	18.5
Accumulative position drift spoofing (0.5 attack ratio)	48.6	2.7	17.9
Emergency stop spoofing with defense algorithm	64.6	2.5	26.2
Accumulative position drift spoofing with defense algorithm	73	2.9	25

deployed in VENTOS. The simulation results of mobility, safety, and environmental sustainability for 39 cases with different CAV penetration rates, V2C ratios, and cyberattack ratios were compared and analyzed. In the worst case, up to a 55.19% decrease in network efficiency was observed. Unlike the scenarios without cyberattacks, cases with higher CAV penetration rates were more susceptible to the presence of attacks, leading to significant system performance degradation. To address this issue, an MMSE-based defense algorithm was proposed and deployed in this study. The simulation results indicated that the proposed defense algorithm can well improve the cyberattack resilience of the system. It can recover most of the benefits from the cooperative merging system under two attack strategies and even performed better than non-CAV scenarios. Note that it is not necessary to base our proposed attack and defense strategies on DSRC, but they applicable to other communication technologies, including cellular V2X.

As a future step, other types of cyberattack risks, such as jamming (DOS or DDOS), black hole, and Sybil, will be devised and evaluated for cooperative highway on-ramp merge scenarios. The cybersecurity performance of other CAV applications will also be investigated, and respective defense strategies should be designed to improve the attack-resilience performance of target CAV systems.

About the Authors

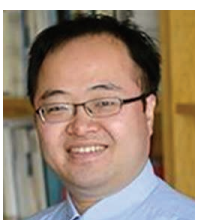


Xuanpeng Zhao (xzhao094@ucr.edu) earned his M.S. degree in electrical engineering from the University of California, Riverside, Riverside, California, 92507, USA, where he is currently a Ph.D. student in electrical engineering. His research focuses on embedded systems, computer vision, and connected and automated vehicle technology.

Ahmed Abdo (aabdo003@ucr.edu) earned his MSEE degree at California State University. He is currently a Ph.D. student in computer engineering at the University of California, Riverside, Riverside, California, 92507, USA. His research interests center around security in automated and autonomous systems, such as connected and self-driven vehicles.

Xishun Liao (xliao016@ucr.edu) earned his M.Eng. degree in mechanical engineering from University of Maryland, College Park. He is currently a Ph.D. student in electrical and computer engineering at University of California, Riverside, Riverside, California, 92507, USA. His research focuses on connected and automated vehicle technology. He is a Student Member of IEEE.

Matthew J. Barth (barth@cert.ucr.edu) earned his Ph.D. degree in electrical and computer engineering from the University of California, Santa Barbara. He is currently the Yeager Families Professor with the College of Engineering, University of California, Riverside, Riverside, California, 92507, USA. He also serves as the director for the Center for Environmental Research and Technology. His current research interests include intelligent transportation systems and the environment, transportation/emissions modeling, vehicle activity analysis, advanced navigation techniques, electric vehicle technology, and advanced sensing and control. He serves as a senior editor for *IEEE Transactions on Intelligent Transportation Systems* and *IEEE Transactions on Intelligent Vehicles*. He served as the IEEE Intelligent Transportation Systems Society (ITSS) president for 2014 and 2015 and is currently the IEEE ITSS vice president for finance. He is a Fellow of IEEE.



Guoyuan Wu (gywu@cert.ucr.edu) earned his Ph.D. degree in mechanical engineering from the University of California, Berkeley. Currently, he holds an associate researcher and an associate adjunct professor position at Bourns College of Engineering—Center for Environmental Research and Technology and the Department of Electrical and Computer Engineering, respectively, in the University of California, Riverside, Riverside, California, 92507, USA. His research focuses on the development and evaluation of sustainable and intelligent transportation system technologies, including connected and automated transportation systems, shared mobility, transportation electrification, the optimization and control of vehicles, traffic simulation, and emissions

measurement and modeling. He is a recipient of the Vincent Bendix Automotive Electronics Engineering Award. He serves as an associate editor for *IEEE Transactions on Intelligent Transportation Systems*, *SAE International Journal of Connected and Automated Vehicles*, and *IEEE Open Journal of Intelligent Transportation Systems*. He is a Senior Member of IEEE and a member of the Vehicle-Highway Automation Standing Committee of the Transportation Research Board.

References

[1] "Global status report on road safety 2018," Geneva, Switzerland: World Health Organization (WHO), 2018, pp. 1–13.

[2] F. Caiazzo, A. Ashok, I. A. Waitz, S. H. L. Yim, and S. R. H. Barrett, "Air pollution and early deaths in the United States. Part I: Quantifying the impact of major sectors in 2005," *Atmos. Environ.*, vol. 79, pp. 198–208, Nov. 2013, doi: 10.1016/j.atmosenv.2013.05.081.

[3] A. Ghiasi, O. Hussain, Z. (Sean) Qian, and X. Li, "A mixed traffic capacity analysis and lane management model for connected automated vehicles: A Markov chain method," *Transp. Res. B, Methodol.*, vol. 106, pp. 266–292, Dec. 2017, doi: 10.1016/j.trb.2017.09.022.

[4] B. Han and R. A. Reiss, "Coordinating ramp meter operation with upstream intersection traffic signal," *Transp. Res. Board*, vol. 3, no. 2, no. 1446, pp. 44–47, 1994, doi: 10.1260/2046-0430.3.2.179.

[5] Z. Wang, G. Wu, and M. J. Barth, "Developing a distributed consensus-based cooperative adaptive cruise control system for heterogeneous vehicles with predecessor following topology," *J. Adv. Transp.*, vol. 2017, 2017, doi: 10.1155/2017/1023654.

[6] J. R. Scariza, "Evaluation of coordinated and local ramp metering algorithm using microscopic traffic simulation," Master's thesis, Dept. of Civil and Environ. Eng., MIT, Cambridge, MA, USA, 2003.

[7] K. Shaaban, M. A. Khan, I. Kim, and R. Hamila, "Queue discharge at freeway on-ramps using coordinated operation of a ramp meter and an upstream traffic signal," *Procedia Comput. Sci.*, vol. 170, pp. 347–353, Apr. 2020, doi: 10.1016/j.procs.2020.03.056.

[8] Z. Zhao, G. Wu, Z. Wang, and M. J. Barth, "Optimal control-based ramp merging system for connected and automated electric vehicles," 2019, *arXiv:1910.07620v2*.

[9] L. C. Davis, "Effect of adaptive cruise control systems on mixed traffic flow near an on-ramp," *Phys. A, Stat. Mech. Appl.*, vol. 379, no. 1, pp. 274–290, 2007, doi: 10.1016/j.physa.2006.12.017.

[10] D. Tian, G. Wu, K. Boriboonsomsin, and M. J. Barth, "Performance measurement evaluation framework and co-benefit\/tradeoff analysis for connected and automated vehicles (CAV) applications: A survey," *IEEE Intell. Transp. Syst. Mag.*, vol. 10, no. 3, pp. 110–122, 2018, doi: 10.1109/MITS.2018.2842020.

[11] J. Reilly, S. Martin, M. Payer, and A. M. Bayen, "On cybersecurity of freeway control systems: Analysis of coordinated ramp metering attacks," 2015.

[12] X. Liao *et al.*, "A game theory based ramp merging strategy for connected and automated vehicles in the mixed traffic: A unity-SUMO integrated platform," 2021.

[13] Z. Sun, T. Huang, and P.-T. Zhang, "Cooperative decision-making for mixed traffic: A ramp merging example," *Transp. Res. C, Emerg. Technol.*, vol. 120, p. 102764, Nov. 2020, doi: 10.1016/j.trc.2020.102764.

[14] M. Hashem Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," *IEEE Veh. Technol. Mag.*, vol. 12, no. 2, pp. 45–51, 2017, doi: 10.1109/MVT.2017.2669348.

[15] F. F. Hassanzadeh and S. Valaee, "Reliable broadcast of safety messages in vehicular ad hoc networks," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2009, pp. 226–234, doi: 10.1109/INFCOM.2009.5061925.

[16] N. Chen, B. Arem, T. P. Alkim, and M. Wang, "A hierarchical model-based optimization control approach for cooperative merging by connected automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 12, pp. 1–14, 2020, doi: 10.1109/TITS.2020.3007647.

[17] J. Rios-Torres and A. A. Malikopoulos, "Automated and cooperative vehicle merging at highway on-ramps," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 4, pp. 780–789, 2017, doi: 10.1109/TITS.2016.2587582.

[18] C. Bhat, "Cybersecurity challenges and pathways in the context of connected vehicle systems," Rep. no. D-STOP/2017/134, 2018.

[19] M. Dibaei *et al.*, "An overview of attacks and defences on intelligent connected vehicles," 2019, *arXiv:1907.07455*.

[20] Q. A. Chen, Y. Yin, Y. Feng, Z. M. Mao, and H. X. L. Liu, "Exposing congestion attack on emerging connected vehicle based traffic signal control," in *Proc. Netw. Distrib. Syst. Security Symp.*, 2018, doi: 10.14722/ndss.2018.23236.

[21] "Multi-modal intelligent traffic safety system (MMITSS)," U.S. Dept. of Transportation. [Online]. Available: https://www.its.dot.gov/research_archives/dma/bundle/mmitss_plan.htm

[22] "Security credential management system (SCMS)," U.S. Dept. of Transportation. [Online]. Available: https://www.its.dot.gov/factsheets/pdf/CV SCMS.pdf

[23] L. Cui, J. Hu, and P. Bujanovic, "Development of a simulation platform for safety impact analysis considering vehicle dynamics, sensor errors, and communication latencies: Assessing cooperative adaptive cruise control under cyber attack," *Transp. Res. C, Emerg. Technol.*, vol. 97, pp. 1–22, Dec. 2018, doi: 10.1016/j.trc.2018.10.005.

[24] P. Wang, X. Wu, and X. He, "Modeling and analyzing cyberattack effects on connected automated vehicular platoons," *Transp. Res. C, Emerg. Technol.*, vol. 115, p. 102625, Jun. 2020, doi: 10.1016/j.trc.2020.102625.

[25] M. Hadded, P. Merdrignac, S. Duhamel and O. Shagdar, "Security attacks impact for collective perception based roadside assistance: A study of a highway on-ramp merging case," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, 2020, pp. 1284–1289, doi: 10.1109/IWCMC48107.2020.9148235.

[26] W. Xu, C. Yan, W. Jia, X. Ji, and J. Liu, "Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 5015–5029, Dec. 2018, doi: 10.1109/JIOT.2018.2867917.

[27] J. Giraldo and A. A. Cardenas, "Moving target defense for attack mitigation in multi-vehicle systems," in *Proactive and Dynamic Network Defense. Advances in Information Security*. Cham, Switzerland: Springer-Verlag, vol. 74, doi: 10.1007/978-3-030-10597-6_7.

[28] D. Liu, P. Ning, A. Liu, C. Wang, and W. K. Du, "Attack-resistant location estimation in wireless sensor networks," *ACM Trans. Inform. Syst. Security*, vol. 11, no. 4, pp. 1–39, 2004, doi: 10.1145/1380564.1380570.

[29] A. Savvides, C. Han, and M. Srivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in *Proc. ACM MobiCom 01*, 2001, pp. 166–179, doi: 10.1145/381677.381693.

[30] K. Benkic, M. Malajner, P. Planinsic, and Z. Cucej, "Using RSSI value for distance estimation in wireless sensor networks based on ZigBee," in *Proc. 15th Int. Conf. Syst., Signals Image Process.*, 2008, pp. 303–306, doi: 10.1109/IWSSIP.2008.4604427.

[31] H. Suo, J. Wan, L. Huang, and C. Zou, "Issues and challenges of wireless sensor networks localization in emerging applications," in *Proc. Int. Conf. Comput. Sci. Electron. Eng. (ICCSEE)*, Mar. 2012, pp. 447–451.

[32] M. Demirbas and Y Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks," in *Proc. Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM'06)*, 2006, pp. 5–pp.-570, doi: 10.1109/WOWMOM.2006.27.

[33] J. Xu, W. Liu, F. Lang, Y. Zhang, and C. Wang, "Distance measurement model based on RSSI in WSN," *Wireless Sensor Netw.*, vol. 2, no. 8, pp. 606–611, 2010, doi: 10.4236/wsn.2010.28072.

[34] VENTOS—VEhicular NeTwork Open Simulator. [Online]. Available: http://maniam.github.io/VENTOS/

[35] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011, doi: 10.1109/JPROC.2011.2132790.

[36] Simulation of Urban MObility. Accessed: Jul. 30, 2020. [Online]. Available: https://www.eclipse.org/sumo/

[37] OMNeT++. [Online]. Available: https://www.omnetpp.org/

[38] L. Li, X. M. Chen, and L. Zhang, "A global optimization algorithm for trajectory data based carfollowing model calibration," *Transp. Res. C, Emerg. Technol.*, vol. 68, pp. 311–332, 2016, doi: 10.1016/j.trc.2016.04.011.

[39] "Definition of vehicles, vehicle types, and routes," SUMO. [Online]. Available: https://sumo.dlr.de/docs/Definition_of_Vehicles,_Vehicle_Types,_and_Routes.html#car-following_models

[40] S. Krauß, H. Mobilitat, and S. Koln, "Microscopic modeling of traffic flow: Investigation of collision free vehicle dynamics," EDTEWEB, 1998. [Online]. Available: https://www.osti.gov/etdeweb/biblio/627062

[41] J. Erdmann, "SUMO's lane-changing model," in *Modeling Mobility with Open Data*, M. Behrisch, M. Weber, Eds., Cham Switzerland: Springer-Verlag, doi: 10.1007/978-3-319-15024-6_7.

[42] M. Kamrani, R. Arvin, and A. J. Khattak, "Extracting useful information from basic safety message data: An empirical study of driving volatility measures and crash frequency at intersections," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 2672, no. 38, pp. 290–301, Dec. 2018, doi: 10.1177/0361198118773869.

[43] "MOVES and other mobile source emissions models," U.S. Environmental Protection Agency, 2019. [Online]. Available: https://www.epa.gov/moves