Anomaly Detection for Cooperative Adaptive Cruise Control in Autonomous Vehicles Using Statistical Learning and Kinematic Model

Faris Alotibi and Mai Abdelhakim

***Abstract*— This paper focuses on Cooperative Adaptive Cruise Control (CACC) in autonomous vehicles. In CACC, vehicles regulate their speed according to a preceding "leader" vehicle in the lane, forming a platoon. In a benign environment, CACC reduces fuel consumption, maximizes road capacity, and ensures traffic safety. However, CACC is vulnerable to various security threats. In this paper, we consider one of the critical threats, where the platoon leader is compromised, and forges acceleration information sent to platoon members. Such attack would lead to traffic instability and potential collisions. First, we propose information sharing in CACC model to allow vehicles and fixed infrastructure to sense and share information about platoon leaders, hence improves the reliability and supports the detection of anomalous behavior. Then, we propose a real-time anomaly detection mechanism that combines statistical learning with the physics laws of kinematics. Specifically, we propose Generalized Extreme Studentized Deviate with Sliding Chunks (GESD-SC) approach, which is applied at each vehicle in the platoon to detect anomalies in real-time based on the vehicle's own speeding decisions. Kinematic model is also utilized to detect unexpected deviations using the leader's information, communicated directly and observed by the leader's neighboring vehicle(s) and/or supporting infrastructure. Combining kinematic model with GESD-SC has shown to be effective in detecting falsification attacks in CACC. Furthermore, we analyze the time performance, and show that the proposed technique outperforms existing method in detection accuracy and processing time.**

***Index Terms*— Statistical learning, CACC, anomaly detection, kinematic model.**

I. Introduction

AUTONOMOUS vehicles revolutionize the operation of transportation systems and bring tremendous benefits to society and environment. Autonomous vehicles are equipped with variety of on-board sensors to gather data about their surrounding environment and make autonomous decisions accordingly [1]. On-board sensors include light detection and range (LIDAR) technology for scanning the environment, global positioning system (GPS) for localization and navigation, and ultrasonic sensors for object detection. The data generated by these sensors are then processed by on-board electronic control units (ECUs) to generate commands to the vehicle's signaling, braking, steering, and acceleration systems [1]. However, autonomous vehicles decisions using local sensors solely have shown to be unreliable [2]–[6]. Because of the driving environment nature, sensors have potential constraints that can affect their ability of obtaining highly accurate measurements. Barriers include weather conditions and line of sight [7].

The limitations of independent and local decision making in autonomous vehicles can be mitigated by information sharing using vehicular communication systems [8], consisting of vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communications [7], [9]–[12]. V2V allows vehicles to create peer-to-peer (P2P) network for exchanging information. V2I allows vehicles to communicate with roadside infrastructures (such as traffic lights, street lights, and roadside units) to exchange relevant information [13]. It is expected that through using local on-board sensors in addition to information exchanged over V2V and V2I, reliable driving experience can be achieved [1], [10], [14].

By enabling communications among vehicles, many applications have been envisioned. Cooperative Adaptive Cruise Control (CACC), which is extended from the typical Adaptive Cruise Control (ACC), is among the most prominent applications of autonomous vehicles. In CACC, multiple connected vehicles are created forming a platoon, which is a stream of vehicles moving as a single unit. This stream consists of a lead vehicle and member vehicles, where the latter dynamically adjusts the speed to match the former; thus, maintaining tightly coupled stream of vehicles [13]. In a benign environment, CACC provides several benefits, such as improving road safety [13], increasing traffic flow rate and highway capacity [15], reducing air pollution as well as energy consumption [16], and hence enhancing fuel efficiency [17]. The study presented in [18] shows that CACC can lead to a reduction in fuel consumption by 37% and CO_2 emissions by 36%. However, before widely deploying CACC, its vulnerabilities to various security threats should be addressed [3], [4], [19], [20]. For example, in [19], authors demonstrated how attacks can create significant instability in the CACC platoons leading to an increase in fuel consumption and traffic

Manuscript received February 1, 2019; revised September 13, 2019 and January 9, 2020; accepted March 9, 2020. The Associate Editor for this article was J. E. Naranjo. *(Corresponding author: Mai Abdelhakim.)*

Faris Alotibi is with the College of Computer Science and Engineering, Taibah University, Medina 42353, Saudi Arabia, and also with the Department of Informatics and Networked Systems, School of Computing and Information, University of Pittsburgh, Pittsburgh, PA 15213 USA (e-mail: fotibi@taibahu.edu.sa; f.alotibi@pitt.edu).

Mai Abdelhakim is with the Department of Electrical and Computer Engineering, Swanson School of Engineering, University of Pittsburgh, Pittsburgh, PA 15261 USA (e-mail: maia@pitt.edu).

Digital Object Identifier 10.1109/TITS.2020.2983392

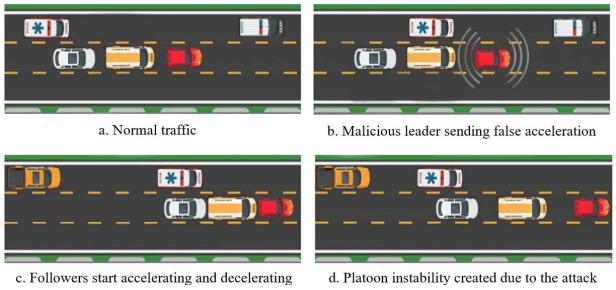


Fig. 1. Acceleration falsification attack scenario. a) middle lane shows a normal platooning. b) the leader begins transmitting falsified information via V2V. c) due to falsified acceleration data, platoon members accelerate/decelerate. d) platoon becomes unstable and has non-uniform gaps as a result of the attack.

deformation. A platoon's leader plays a key role in maintaining the safety and efficiency of CACC. It is critical to ensure that platoons are not led by compromised vehicles.

In this paper, we focus on one of the most difficult threats in CACC, where the platoon leader is compromised and disseminates falsified acceleration information to platoon members. Such attack would potentially lead to traffic congestion, potential collisions, and/or platoon and flow instability as shown in Fig. 1. It is worth noting that, since such attack originates from a vehicle that is authentic, yet compromised, in the platoon, cryptographic means would not be able to resolve it. As an effort to solve this problem, first, we propose information sharing in CACC model, where vehicles (not necessarily members of the platoon) and the fixed infrastructure collaborate to sense and share critical information about platoon leaders (e.g. location and velocity). That is, we utilize local sensors, V2V, and V2I to enable information about platoon leaders to be monitored and shared with platoon members; hence allowing platoon members to accurately detect anomalies. Whenever a platoon member identifies a suspicious behavior, it reports to the infrastructure. This information can be stored in the cloud to enable tracking of vehicles' trust/reliability, which should be validated before a vehicle leads or joins a platoon in the future.

Then, we propose a real-time anomaly detection mechanism that combines the statistical Generalized Extreme Studentized Deviate (GESD) approach with the physical laws of kinematics. In the statistical approach, we propose GESD with Sliding Chunks (GESD-SC), which is applied at each vehicle in the platoon to detect anomalies in real-time based on the vehicle's own speeding decisions. In GESD-SC, a chunk is a window of a predefined number of speed observations; after the initial chunk, the window slides in each time step and outliers are detected by the GESD algorithm. GESD-SC requires the knowledge of the vehicles' own speeding observations only, which are determined based on several parameters including the leader's reported acceleration information. On the other hand, the kinematic model (based on physics laws of kinematics) is utilized to detect unexpected deviations in behavior. We use the leader's transmitted acceleration along with its velocity and position observed by the leader's neighboring vehicle(s) and/or supporting infrastructure. Combining the kinematic model with GESD-SC has shown an effective capability in identifying data manipulation attacks launched by a compromised leader vehicle in CACC. We utilize python and VENTOS for simulation and illustrate that the proposed mechanism accurately detects more than 92% of anomalies with less than 13% false alarms. We also evaluate the computation time of the combined approach for different chunk sizes. We compare the performance with existing approach and illustrate that the performance of the proposed mechanism is superior in both computation time and detection accuracy.

II. Related Work

Despite the pivotal benefits of CACC application, there has been very limited attempts to address its security concerns. CACC is susceptible to multiple attacks, including external and internal threats. The external threats are launched by unauthenticated entities. For instance, an external attacker can jam the communications channel used for V2V; hence, disrupting the data exchange between vehicles [19]. Several existing methods attempt to secure the communications in vehicle to everything (V2X) (includes V2V and V2I). For example, the work in [21] and [22] utilize cryptographic techniques to defend against external attacks. Other attacks could target the vehicles' on-board sensors by manipulating or distorting their readings, which would lead to traffic instability as demonstrated in [2], [5]. On the other hand, internal threats are more challenging to detect and counteract given that they are launched by authenticated entities in the system. Compromised entities can perform a wide range of attacks, such as data falsification, spoofing, Denial-of-Service (DoS), etc. So far, little attention has been given to internal threats in autonomous vehicles.

For secure operation, it is crucial that autonomous vehicles be capable of detecting and responding to threats. Anomaly detection mechanisms have been extensively studied in the literature. Some of them use the power of machine learning, whereas others rely on modeling methods. In [23], authors studied threats in vehicular platoons. They proposed a model-based detection scheme and global reputation scheme to detect malicious vehicles. The scheme assumes that the leader vehicle is benign while other platoon members could be compromised. Then it relies on the platoon leader to model the behaviors of platoon members. The scheme would fail to detect malicious vehicles in the existence of a compromised leader. The malicious leader problem was considered in [24], where authors presented a statistical learning approach to detect a platoon leader's abnormal behaviors. The scheme, which we refer to as ESD-S, incorporates Extreme Studentized Deviate (ESD) and Seasonal and Trend decomposition using Loess (STL) to detect anomalies. In particular, STL is used to extract the seasonal feature of the speed observations. The median of the observations is also computed. Then, both the seasonal and the median are subtracted from the observations, and ESD is applied on the residual to detect outliers. The scheme would not be able to perform anomaly detection in real-time, as it needs to obtain a set of new observations before it can detect an attack. This waiting time opens a window for

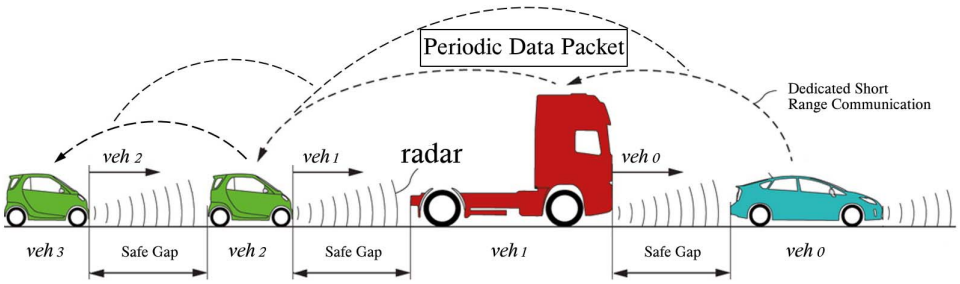


Fig. 2. Utilizing on-board sensor and communication capability in CACC platoon system model.

a malicious vehicle to launch the attack and negatively impact the platoon. Performance evaluation was not thoroughly presented in [24]. In [25], Hidden Markov Model (HMM) and physics-based techniques are proposed for threat detection in CACC, where each vehicle validates its direct preceding vehicle behavior. The HMM approach requires processing power, more storage, and training data, which could render it impractical in a time-sensitive application, such as CACC. In [26], we applied physics laws of kinematics and data fusion to detect anomalies. In this paper, we focus on securing CACC through utilizing both statistical learning and kinematic model.

We develop anomaly detection mechanism in CACC, which can be applied in real-time. We employ both kinematic model and statistical based approaches in order to examine the statistical dependencies in the data as well as the intrinsic dynamics that the system is expected to follow. The statistical learning allows each platoon member to analyze its own autonomously selected velocity, which is influenced by the acceleration data received from the platoon leader. We modify the typical application of GESD by using sliding chunks that enable the detection mechanism to be carried out in real-time, without the need to wait for several new observations before a decision is made. The mechanism also incorporates validation using the kinematic model to examine the leader's behavior. The kinematic model is applied in a similar way as in [25], however we focus on validating the behavior of the platoon leader, which plays a key role in safety and efficiency of CACC. Applying the kinematic model at each node to examine the behavior of the platoon leader requires information about the leading vehicle's speed and location. This information can be obtained through the proposed information sharing model. We show that combining the kinematic model with GESD-SC achieves an improved performance over any of them individually and over the existing ESD-S technique in [24].

III. Proposed System Model

A. Overview of Platooning in CACC

In CACC, vehicles utilize observed and shared information to adjust their speed cooperatively [27]. Each vehicle has sensing devices and communications capabilities to collect and share information with other vehicles. Communications in vehicles can be made over direct and secure communication links. Such links can be established using dedicated short-range communications (DSRC)/IEEE 802.11p protocol[1] [29] or cellular vehicle-to-everything (C-V2X)/5G technology [30]. Using CACC, vehicles form a platoon as shown in Fig. 2. A platoon is a collection of vehicles that moves as a single unit. It is particularly useful on highways. A platoon is composed of a leader vehicle in the front and multiple platoon members following the leader. In CACC platoon management protocol, different network topologies have been proposed, such as predecessor-leader (P-L) and predecessor-follower (P-F) topologies. Here, the P-L topology is adopted [31] as it allows a platoon leader to directly communicate with all platoon members. This topology is more reliable and less impacted by error propagation than P-F topology, where a vehicle in a platoon only communicates with its direct succeeding and preceding vehicles [32].

The platoon leader periodically broadcasts messages containing information, such as platoon identifier, acceleration, position, velocity, maximum deceleration, etc., to platoon members. Such information is provided in cooperative awareness messages (CAMs) according to the European Telecommunications Standards Institute (ETSI) [33] or in basic safety messages (BSMs) according to the US SAE J2735 standard [34]. For simplicity, these messages are referred to as beacon messages. Platoon members adjust their speed according to the received and sensed information. More specifically, to determine the speed value, each vehicle utilizes the leader's acceleration obtained from the transmitted beacon messages, and the preceding vehicle's position and velocity obtained by local sensors (not the ones in the beacon) [25].

Let a platoon be composed of N vehicles, veh_i denotes the ith vehicle in the platoon, where $i \in [0, N-1]$. veh_0 is the leading vehicle and veh_1 to veh_{N-1} are the remaining members. The platoon's vehicles are assumed to be driving in a straight lane as depicted in Fig. 2, which is a CACC typical driving model [23]. Members of the platoon first compute the distance, known as the safe space gap, that needs to be maintained between each veh_i and its preceding veh_{i-1} in the platoon to avoid collision. According to [27], the safe space gap computed at veh_i, $\forall i \in [1, N-1]$ is determined by

$$g_{i,t_j,safe} = 0.1(v_{i,t_j}) + \frac{v_{i,t_j}^2}{2D_i^{max}} - \frac{v_{i-1,t_j}^2}{2D_{i-1}^{max}} + 2.0, \qquad (1)$$

[1]DSRC has a dedicated spectrum for V2X communications over short range (around half a mile) and supports information exchange between mobile vehicles moving at speed up to 124 m/h [28].

TABLE I
PARAMETERS DESCRIPTION

Parameters	Description
a_{i,t_j}	Acceleration at veh_i at time t_j
K_a	Predefined positive-gain constant for acceleration
K_v	Predefined positive-gain constant for velocity
v_{i,t_j}	Velocity at veh_i at time t_j
K_g	Predefined positive-gain constant for gap
g_{i,t_j}	Instantaneous space gap at veh_i at time t_j
G_{min}	Predefined minimum space gap
T_g	Desired time gap
$g_{i,t_j,safe}$	Safe space gap at veh_i at time t_j
D_i^{max}	Maximum deceleration at veh_i
K_{sc}	Speed control gain constant
$a^p_{i,t_{j+1}}$	Acceleration based on safe-space gap at veh_i
$a^l_{i,t_{j+1}}$	Desired acceleration based on leader's information at veh_i

where ${v_{i,t_j}}^2$ and D_i^{max} are the vehicle's own velocity at time t_j and maximum deceleration, respectively, v_{i-1,t_j} and D_{i-1}^{max} are the preceding vehicle's velocity at time t_j and maximum deceleration, respectively. g_{i,t_j} denotes the space-gap between veh_i and its preceding veh_{i-1}. veh_i should have $g_{i,t_j} \geq g_{i,t_j,safe}$ at any time t; otherwise, veh_i activates the collision avoidance mode, in which it switches to the typical ACC and operates solely on its local sensors, and decelerates by D_i^{max} to avoid a crash.

Accordingly, the acceleration that ensures a safe-space gap between vehicles, $(a^p_{i,t_{j+1}})$, is locally determined at each vehicle veh_i, $\forall i \in [1, N-1]$ in the platoon such that [27]

$$a^p_{i,t_{j+1}} = K_a a_{i-1,t_j} + K_v(v_{i-1,t_j} - v_{i,t_j}) + K_g(g_{i,t_j} - G_{min} - v_{i,t_j} T_g), \quad (2)$$

where a_{i-1,t_j} is the acceleration at veh_{i-1} at time t_j, K_a, K_v and K_g are predefined positive-gain constants for acceleration, velocity, and gap, respectively; g_{i,t_j} is an instantaneous space gap at veh_i at time t_j, G_{min} is a predefined minimum space gap, and T_g is the desired time gap.[3] On the other hand, as vehicles receive information from the platoon leader, the desired acceleration value is determined at each vehicle veh_i in the platoon as [27]

$$a^l_{i,t_{j+1}} = K_{sc}(v_{i=0,t_{j+1}} - v_{i,t_j}), \quad (3)$$

where K_{sc} is a speed control gain constant, $v_{i=0,t_{j+1}}$ is the targeted leader's velocity (computed using its acceleration and time difference), and v_{i,t_j} is the current velocity of veh_i.[4] Overall, based on (2) and (3), the adopted acceleration value is determined at each vehicle veh_i in the platoon by

$$a_{i,t_{j+1}} = min(a^p_{i,t_{j+1}}, a^l_{i,t_{j+1}}), \quad (4)$$

Hence, if the speed determined based on the information from the leader would violate the safe-space gap, the vehicles will determine their speed locally to maintain the safe gap and ensure safety. For better readability, we added the description of these parameters in Table I.

[2]Note that t_j is the instantaneous time.

[3]According to [27], the constants are set to $K_a = 0.66$, $K_v = 0.99s^{-1}$, $K_g = 4.08s^{-2}$, $G_{min} = 2m$, $T_g = 0.55s$.

[4]The speed control gain is set to $K_{sc} = 0.4\ s^{-1}$ [27].

B. CACC Model With Proposed Information Sharing

In CACC, platoon members make speeding decisions based on their local sensors readings and information sent by the platoon leader. In the existing model, platoon members trust the platoon leader. A major limitation of this is that if platoon's leader is compromised or/and the communication link between the leader and platoon members is compromised, wrong decisions would be made, potentially impacting the platoon stability and safety on the road. Since platoon leader plays a significant role in ensuring platoon's stability, safety, and efficiency, its behavior must be verified during platooning. For high-confidence decisions, we propose information sharing in a CACC model to allow the driving behavior of a platoon leader to be verified through multiple sources (infrastructure and vehicles) and shared with platoon members (through V2I and V2V). A cloud can also be used to store platoon leaders' identities and trust for profiling [35].

We exploit fixed infrastructure employing sensing and communications capabilities, for example through Road Side Units (RSUs) [36], which can monitor and transmit vehicles' speed and position to platoon members, as shown in Fig. 3. There are several existing efforts that focus on improving the reliability of communications between vehicles and infrastructure. In [37], authors developed a probabilistic approach to choose an overlapping proportion between RSUs' coverage to ensure a communication with high reliability and limited interference. Authors in [38] proposed reliable V2X short range communications solution based on the cellular long-term evolution (LTE) technology. For a higher reliability, utilizing both DSRC and cellular communications was proposed for V2X in [39]. Here, we assume that the infrastructure can measure and communicate leader's speed and position reliably.

Relying solely on RSUs may not be sufficient, as they may not be always available, and their detection accuracy may face challenges when vehicles travel at high velocity. In addition to the fixed infrastructure, we propose that vehicles on the road collaborate to monitor neighboring platoon leaders and share their information (speed/position) with platoon members in proximity. In particular, the second vehicle in the platoon (succeeding the leader) can identify the speed and location of the leader through its local sensors. This information can then be shared with other platoon members through direct communication links (e.g. DSRC or 5G). For instance, veh_1 in Fig. 3 measures veh_0 (leader) velocity and position using its on-board sensors, then transmits this sensed information to the platoon members (they may not observe the leader's dynamics using their own sensing devices due to the line of sight constraint). Same information can be obtained from other vehicles on the road, not necessarily members of the platoon, such as NV_0 and NV_1 (neighboring vehicles) in Fig. 3 that can decode the beacon messages from the leader and detect leader's position/speed through local sensors.

Overall, platoon members receive information about the leader's position and velocity from their local sensors (if applicable), from vehicles on the road, and from the fixed infrastructure. Data fusion can then be used to fuse such information and obtain more accurate approximation of the leader's position and speed [26]. Then, with that accurate

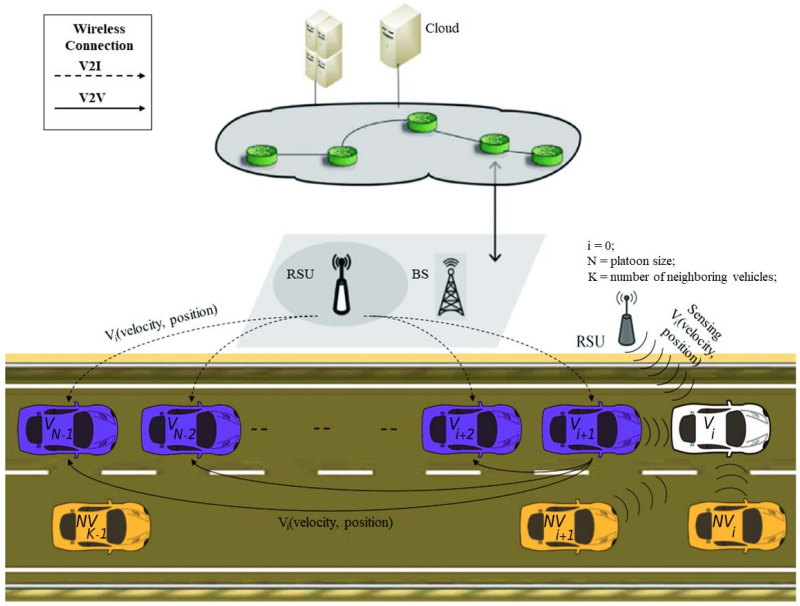


Fig. 3. Proposed information sharing where sensing and sharing of platoon leader's position and velocity are used in CACC model.

estimation, anomaly detection scheme is applied as will be described in the following section. Errors in measurements from each source can be learned and taken into account during fusion (corrected or weighted for example by weighted average). Existing fusion techniques can be examined and applied. In this paper, however, we focus on how to utilize such information to detect anomalies in the platoon leaders' behavior assuming that the leader's position and speed can be accurately obtained after fusion.

We propose to use the cloud-based trust management system [40] to track the reliability of platoon vehicles. That is, whenever a platoon member identifies a suspicious behavior, it reports to the infrastructure its detection information. This information is then stored on the cloud to track vehicles' trustworthiness. Revocation of suspicious vehicles from the platoon membership is initiated if the trust is below a certain level. In addition, trust/reliability of vehicles has to be verified before a vehicle leads or joins a platoon in the future.

IV. Attack Model and Effect on CACC

A. Model of Attack

In this paper, we consider one of the most challenging threats to CACC, which is a compromised platoon leader that falsifies and transmits the acceleration information in beacon messages. Recall that platoon members utilize this acceleration information to adapt their speeding behavior as described in Section III. This type of attack would lead to increase in fuel consumption, passengers' discomfort, platoon instability, and potential collisions. We adopt the falsification model in [25], which is an oscillation that is difficult to detect, as values fluctuate within a small range ($-5m/s^2$ to $5m/s^2$). The falsified acceleration $a_{falsified,t_j}$ can be expressed as

$$a_{falsified,t_j} = a_{original,t_j} + m_a * sin(f * t_j), \tag{5}$$

where $a_{original,t_j}$ is the current true acceleration before manipulation, m_a is the magnitude of falsification, f is the frequency of the sinusoid, and t_j is the current time.

B. Impact of Attack

The severity of the attack can be measured by three metrics: passenger discomfort, waste, and crash [25], as described below.

Stability and Passenger Comfort: Platoon stability can be measured by the amplification of any error in vehicles' position/velocity [31]. When a platoon is stable, passengers' discomfort is minimized to approximately zero. One way to measure passengers' discomfort is by measuring the rate of change in the acceleration with time. That is, for veh_i, the discomfort can be expressed as

$$discomfort_i = da_i/dt. \tag{6}$$

To get an assessment of passengers' discomfort over a running platoon in CACC mode, we use the maximum $discomfort$ over all time steps.

Efficiency: To increase efficiency, CACC tries to maintain fixed distance between platoon members (determined by the safe gap). That will increase road capacity, which is one of the prominent advantages of CACC. Thus, a platoon of vehicles in CACC mode is efficient if the wasted distance is minimized. The waste can be expressed as

$$waste_i = \int_{t=0}^{t_{end}} \left(g_i^t - g_{i,safe}^t \right) * dt, \tag{7}$$

where g_i^t is current time gap, given by $g_i^t = g_{i,t_j}/v_{i,t_j}$ at time $t = t_j$, and $g_{i,safe}^t$ is safe time gap, given by $g_{i,safe}^t = g_{i,t_j,safe}/v_{i,t_j}$. We compute the waste from the platoon's beginning (at $t = 0$) until end (t_{end}).

Safety: At any time t, the platoon is considered *safe* when the instantaneous time-gap g_i^t between every veh_i and its preceding veh_{i-1} is greater than or equal to $g_{i,safe}^t$. The safety is measured through finding the percentage of violation of g_i^t to the gap $g_{i,safe}^t$. Crash metric for each veh_i can be defined as [25]

$$crash_i = max\left\{0, max_t\left\{0, \frac{g_{i,safe}^t - g_i^t}{g_{i,safe}^t}\right\}\right\} * 100. \quad (8)$$

V. Proposed Attack Detection With GESD and Kinematic Model

In this section, we present our proposed anomaly detection mechanism. The proposed mechanism incorporates both statistical learning and kinematic model to identify anomalies. We first describe the proposed GESD-SC, then present how we apply the kinematic model in CACC. Finally, we illustrate the combined method.

A. GESD With Sliding Chunks (GESD-SC)

GESD is a popular statistical technique that is used to identify arbitrary number of outliers in observations assuming a univariate and approximately normally distributed data. In [41], authors showed that the typical speeding behaviors of a vehicle on highway over a specific period of time tend to be normally distributed. An upper bound on the number of potential outliers, which we denote as r, is provided to the GESD approach. Given r, the GESD algorithm executes a number of hypothesis tests, starting with a test of one outlier up to a test of r outliers [42]. After each test, the sample that is far from the mean of observations is discarded, and statistics are computed with the remaining observations. Then, the process is repeated for all tests. A test statistics is computed for the r tests, and based on a predefined significance level α, anomalous observations (outliers) are determined. Here, we apply GESD to detect outliers in CACC platooning.

We propose GESD-SC to detect anomalous behavior in real-time, which is essential in time-sensitive applications as CACC. In GESD-SC, each vehicle applies GESD to a chunk, which is a sliding window of the vehicle's own speeding observations, denoted as C_V. Let the chunk size be w observations. Hence, $C_V = V_0, V_1, \ldots V_{w-1}$. Initially, the chunk is composed of the first w samples of the vehicle's own velocity upon joining the platoon, i.e., for veh_i, $V_{i,t_j} = v_i$ at time slot t_j. This window slides each time step, and outliers are detected in each time step using the GESD algorithm. Specifically, if there is no outliers, the vehicle shifts the window by one sample, discards the oldest speeding observation and adds the new observation (computed upon the arrival of the new acceleration information from the leader) into the wth chunk's position.

If outliers are detected within a chunk, they are discarded. In addition to the new observation that is added to the sliding chunk, more observations can also be added if needed to complete the window of w observations. GESD-SC ensures that anomalies can be detected in real-time as will be shown in Section VI. The proposed algorithm is described in Algorithm 1.

Algorithm 1 Anomaly Detection Using GESD-SC

Input: Initial observations N_w, chunk size w, significance level α, number of potential outliers r, new velocity v_i

Output: Vector of detected anomalies AV_{GESD}

Initialization: Assign $C_V = N_w = V_0, V_1, \ldots V_{w-1}$

1: $X_A = GESD\ (C_V, r, \alpha)$, is detected anomalies in C_V
2: Add X_A to anomalous velocity vector, AV_{GESD}.
3: Slide chunk: $V_i = V_{i+1}, \forall i \in \{0, w-2\}$, and $V_{w-1} = v_i$
4: repeat 1, 2, 3
5: **return** AV_{GESD}.

B. Applying Kinematic Model for Anomaly Detection

In addition to the GESD-SC, we also utilize the kinematic model for real-time anomaly detection. Applying the kinematic model relies on the information sharing described in Section III, where data is obtained from different sources. First, the model utilizes the acceleration values, denoted by a_{i,t_j} and $a_{i,t_{j-1}}$,[5] transmitted consecutively at two time steps t_j and t_{j-1} by the platoon leading vehicle. Then the algorithm needs to obtain the velocity and position of the leading vehicle, which are exchanged collaboratively through information sharing with neighboring vehicles (including the platoon second vehicle) and/or the infrastructure, as well as vehicles' on-board sensing devices if applicable. Recall that if a vehicle determines the position and velocity of the leader through local sensors, it sends this information via direct links (e.g. DSRC) to platoon vehicles.

We use physics laws of kinematics to validate the behavior of the platoon leader. Let the velocity of the platoon leading vehicle at t_j and t_{j-1} be denoted as v_{i,t_j} and $v_{i,t_{j-1}}$, respectively. Similarly, the position of the leader at time t_j and t_{j-1} is denoted as p_{i,t_j} and $p_{i,t_{j-1}}$, respectively. We represent the position in one dimension since the platoon is assumed to be in a particular lane. Let Δt be the difference in time between t_j and t_{j-1}, $v_{min} = min(v_{i,t_{j-1}}, v_{i,t_j})$ is the minimum velocity, $v_{max} = max(v_{i,t_{j-1}}, v_{i,t_j})$ is the maximum velocity, $a_{min} = min(a_{i,t_{j-1}}, a_{i,t_j})$ is the minimum acceleration, $a_{max} = max(a_{i,t_{j-1}}, a_{i,t_j})$ is the maximum acceleration. Let Δp be the difference in position between p_{i,t_j} and $p_{i,t_{j-1}}$, i.e., $\Delta p = |p_{i,t_j} - p_{i,t_{j-1}}|$, and Δv be the difference in velocity between v_{i,t_j} and $v_{i,t_{j-1}}$, i.e., $\Delta v = |v_{i,t_j} - v_{i,t_{j-1}}|$. Then, to validate the behavior of the platoon leader, each platoon member should ensure that the following conditions are true at each time instance:

$$\Delta p \geq disp_{min}, \quad \Delta p \leq disp_{max}, \quad (9)$$

$$\Delta v \leq V_{maxGain}, \quad \Delta v \geq V_{minGain}, \quad (10)$$

where $disp_{max}$ is the maximum displacement, $disp_{min}$ is the minimum displacement, $V_{maxGain}$ is the velocity maximum gain, and $V_{minGain}$ is the velocity minimum gain [25].

[5]Here index $i = 0$ refers to the leader veh_0. So, $a_{i,t_j} = a_{i=0,t=t_j}$. Also. t_j and t_{j-1} refer to current and previous time t, respectively

Algorithm 2 Anomaly Detection Using Kinematic Model

Input: Velocity(v_{i,t_j},$v_{i,t_{j-1}}$), position(p_{i,t_j},$p_{i,t_{j-1}}$), acceleration(a_{i,t_j},$a_{i,t_{j-1}}$), tolerance($error_v$,$error_p$), time(t_j,t_{j-1})

Output: Vector of identified anomalies $AV_{physics}$

Compute Δv, Δp, Δt, v_{max}, v_{min}, a_{max}, a_{min}, $V_{maxGain}$, $V_{minGain}$, $disp_{max}$, and $disp_{min}$.
if $(\Delta p > disp_{max})$ **then**
  Add the new velocity observation V_{i,t_j} to $AV_{physics}$.
else if $(\Delta p < disp_{min})$ **then**
  Add the new velocity observation V_{i,t_j} to $AV_{physics}$.
else if $(\Delta v > V_{maxGain})$ **then**
  Add the new velocity observation V_{i,t_j} to $AV_{physics}$.
else if $(\Delta v < V_{minGain})$ **then**
  Add the new velocity observation V_{i,t_j} to $AV_{physics}$.
end if
return $AV_{physics}$.

From the physics laws of kinematics, we set

$$\begin{aligned} disp_{max} &= v_{max} * \Delta t + 0.5 * a_{max} * \Delta t^2 + error_p, \\ disp_{min} &= v_{min} * \Delta t + 0.5 * a_{min} * \Delta t^2 - error_p, \\ V_{maxGain} &= a_{max} * \Delta t + error_v, \\ V_{minGain} &= a_{min} * \Delta t - error_v, \end{aligned}$$

where $error_p$ and $error_v$ represent possible fluctuations due to noise in measurements. If any of the equations (9)-(10) is not satisfied, the platoon leader being observed is then flagged as suspicious. The kinematic model (physics-based) algorithm is described in Algorithm 2.

It is noted that applying the kinematic model for detecting anomalies is computationally light and requires limited storage space, since only velocity, position, and acceleration in two time instances are needed. However, the accuracy of detection depends on the setting of $error_p$ and $error_v$ and would fail to detect attacks that are hard to distinguish from normal noise.

C. Combining Statistical GESD-SC and Kinematic Model

Each of the above anomaly detection techniques (GESD and kinematic model) has its own limitations. The GESD requires setting an upper bound on the number of anomalies and may not be accurate when the speed observations are not normally distributed. On the other hand, the kinematic model depends on the accuracy of the measurements and the noise thresholds as mentioned earlier. We propose to combine both techniques to improve the detection accuracy.

As illustrated in Fig. 4, the statistical GESD-SC obtains the suspicious speeding decisions, which were obtained based on the acceleration reported by the leader. Each vehicle executes algorithm 1 to identify anomalies and stores the output into a vector AV_{GESD}. Similarly, the kinematic model is validated by taking the new and old velocity and position sensed by neighboring infrastructure or vehicles' local sensors, and the new and old acceleration transmitted by the leader vehicle. Algorithm 2 is also used to detect anomalous observations, represented by a vector $AV_{physics}$. The final anomalous set is

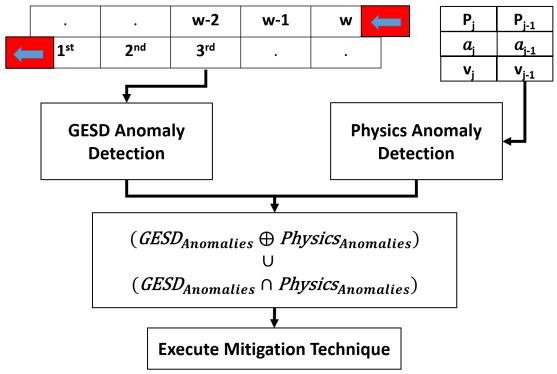


Fig. 4. Proposed anomaly detection mechanism workflow.

then the union of both AV_{GESD} and $AV_{physics}$. If the number of detected anomalies exceeds a certain threshold, the vehicle then splits from the platoon and switches to regular ACC. The threshold is a design parameter that has to take into account possible false alarms of the detection algorithm, and should be designed to reduce traffic disruption.

It is noted that the security improvement enabled by the information sharing model and anomaly detection algorithm will come at the expense of increased overhead and processing time. This sheds light on the trade-off between security and efficiency in autonomous vehicles.

VI. Performance Evaluation

In this section, we illustrate the impact of the data falsification attack launched by a platoon leader in CACC. Then, we assess the accuracy of our proposed mechanism and compare it with existing method.

We use VENTOS (Vehicular Network Open Simulator) to generate traffic data of a CACC platoon. It is an integrated simulator consisting of multiple modules such as SUMO (Simulation of Urban Mobility) and OMNET++/Veins (Vehicles in Network Simulation) [27]. SUMO and OMNET++ are used to simulate our traffic and the wireless communications respectively [43]. For V2V communications between vehicles in CACC mode, IEEE 802.11p wireless protocol is used. Recall that the topology assumed is P-L network topology, in which the leader communicates with each vehicle in the platoon directly over a single hop [36]. After the data is generated by VENTOS, we use python to implement our proposed detection mechanism. Ubuntu 16.4 OS with Intel core i5 CPU processors is used to run the simulations. In the simulation, the platoon runs for 325 time steps, where a time step is 0.10s. To accommodate the frequency of the acceleration messages (less than 100ms), the time step parameter is chosen. We assume the road is 90km length with rightmost lane being reserved for platooning. The platoon consists of five homogeneous and fully automated self-driving vehicles, veh_0 to veh_4, where veh_0 is the platoon leader. Note that the number of vehicles in the platoon will not impact the performance of the proposed detection scheme since P-L topology is assumed. Table II includes other simulation parameters.

We assume that the platoon leader follows the road speed limit. Other platoon members adapt their speed based on

TABLE II
SETTINGS PARAMETERS

Simulation		CACC	
Parameter	**Value**	**Parameter**	**Value**
Simulation Time	325s	Intended Speed	15m/s
Communication Frequency	10Hz	Maximum Speed	20m/s
Vehicle Length	5m	Maximum Acceleration	3m/s^2
Number of Vehicles	5	Maximum Deceleration	5m/s^2
IEEE 802.11p Range	300m	Minimum Speed	5m/s
Chunk Size (w)	10	Platoon Size	5
Platooning Starting Time	10s	Minimum Safe Gap	2m

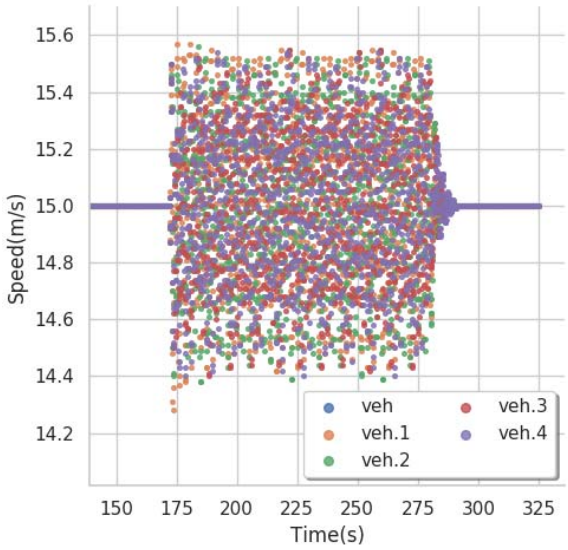


Fig. 5. Each vehicle speeding behavior as a function of time (in seconds). The data manipulation attack begins at t = *172s* and stops at t = *280s*. Figure illustrates the attack influence on the traffic speeding behavior.

the exchanged messages transmitted by the leader via the wireless communications. The objective is to keep following the leader's speed and maintain a constant inter-vehicular space gap in the platoon. We consider only a malicious platoon leader that manipulates the acceleration field in the exchanged messages, as described in Section IV. During the time interval from t = *172s* to t = *280s*, the leader starts sending false information to the platoon members. The acceleration value is manipulated by adding a sinusoidal function with a magnitude m_a =5 m/s^2 and frequency f =5 Hz. The true speed begins from 0m/s and reaches 15m/s, where it remains constant until the end of the simulation.

A. Impact of Attack

Fig. 5 illustrates the speeding decisions of platoon members while the attack is active. As can be seen, traffic instability immediately occurs once the falsification attack begins at t = *172s*. From Fig. 5, it is obvious that the speeding behavior fluctuates around the leader's velocity. The fluctuation of vehicles' speed results from the discrepancy between the leader's claimed and actual acceleration. Consequently, the followers keep changing their speed more frequently to mimic the leader's next speed. The impact of the attack is measured through the discomfort, waste, and crash metrics described in Section IV. Results are shown in Table III, where we take the maximum value of discomfort and the total waste over time for all vehicles in the presence and absence of attack.

TABLE III
DISCOMFORT AND EFFICIENCY METRICS

Vehicles		**1**	**2**	**3**	**4**
No Attack	Discomfort(m/s^3)	0.4	0.7	0.8	1.9
	Waste(s)	189.3	189.2	189	188.8
Acceleration Attack	Discomfort(m/s^3)	17.1	12.9	14.6	15.9
	Waste(s)	191	190.2	190	190

It is shown that the attack has negative impact on passengers' comfort (measured by discomfort) and road efficiency (measured by waste) for all vehicles. It is observed that veh_1 has the largest waste and discomfort, since its speeding behavior is affected by both the leader's steady speed and the falsification attack. Other vehicles' efficiency and passenger discomfort were also affected. This indicates that the resulting negative impact of the attack propagates throughout the platoon. The attack did not lead to any collision ($crash_i = 0, \forall i$) as the vehicles maintained the safe space gap by utilizing their local radar sensors to measure the distance. When the distance between a veh_i and its preceding veh_{i-1} approaches the limits of the safe space gap, veh_i applies the maximum deceleration to avoid collision and maintains the gap using the locally determined acceleration. Nonetheless, we expect that other attack settings or types could result in collisions, for example if the local sensors are also compromised. We intend to consider other attack scenarios in future work.

B. Detection Evaluation

We evaluate the performance of three anomaly detection mechanisms: the proposed GESD-SC only, kinematic model (physics-based) only, and the combined GESD-SC and kinematic model (GESD-physics). The detection approach is applied at each vehicle. We evaluate the three mechanisms based on their detection rate and false alarm rate. Table IV summarizes the performance of the three approaches.

For the GESD-SC, described in Section V, we set the upper bound on the number of potential anomalies to be equal to the chunk size w, where w = 10, and the significance level of the GESD is set to α = 0.05. With the GESD-SC approach solely, the miss detection rate (1 - detection rate) and false alarm rate are around 11% and 12%, respectively, for different vehicles, as shown in Table IV. Note that GESD would suffer from masking and swamping effects [42], when the number of outliers is larger or smaller than the predefined upper bound r, respectively. This could result in misdetection or false alarms. Some false alarms are also attributed to the statistical differences found in observations when vehicles joined a platoon. Upon joining the platoon, vehicles' initial chunks tend to have different speeding observations, which would increase the variability within the chunk as the platoon starts.

Next we apply the kinematic model (physics-based) solely, as described in Section V. We set the tolerance parameters $error_v = 0.1m/s$ and $error_p = 0.15m$. As can be seen in

TABLE IV
DETECTION AND FALSE ALARM RATES FOR ALL VEHICLES

Vehicles		1	2	3	4
False Alarm	GESD-SC	0.09	0.123	0.13	0.142
	Physics	0	0	0	0
	Combined GESD-SC & Physics	0.09	0.123	0.13	0.142
Detection[a]	GESD-SC	0.893	0.892	0.893	0.893
	Physics	0.672	0.672	0.672	0.672
	Combined GESD-SC & Physics	0.92	0.924	0.932	0.92

[a]The attack is executed with $m_a = 5m/s^2$ and $f = 5Hz$.

TABLE V
DETECTION AND FALSE ALARM RATES COMPARISON BETWEEN PROPOSED ALGORITHM AND ALGORITHM IN [24]

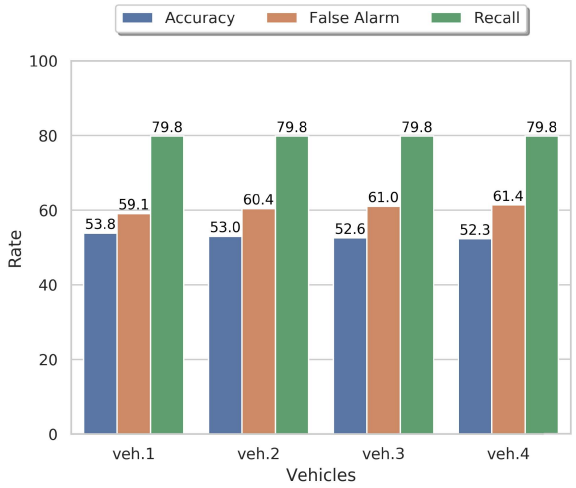
Algorithm	*ESD-S [24]*	*GESD-physics*
False Alarm Rate	0.604	0.121
Detection Rate	0.798	0.924

Table IV, the physics-based approach achieves a zero false alarm rate but very low detection accuracy. The results show that the mechanism fails in detecting 33% of anomalies, which is significant and would be intolerable given the ramifications the anomalies can cause.

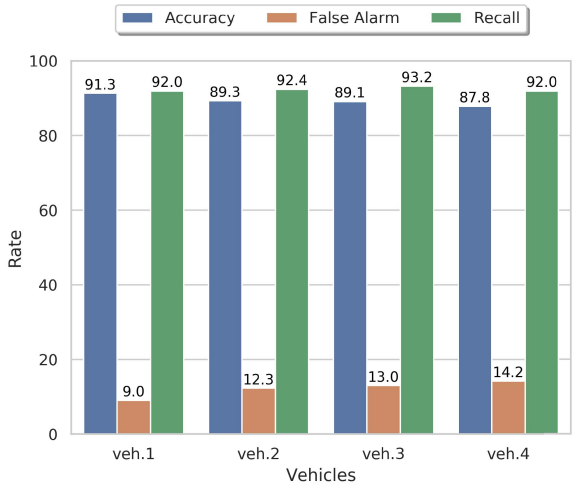
In the proposed combined GESD-physics approach, described in Section V, we use the same settings specified earlier. The combined approach shows a significant improvement in the detection accuracy and the false alarm rate. The detection accuracy at the vehicles ranges from 92% to 93%, and the false alarm is kept low and ranges from 9% to 14%. The combined approach leverages the power of both schemes; the GESD-SC detects small deviations that the physics-based techniques could not detect. Also, the physics-based technique can detect anomalies that the GESD-SC fails to identify from statistical tests.

We compare the proposed combined GESD-physics approach with the scheme presented in [24], which uses the typical ESD with non-overlapping (not sliding) chunks and utilizes STL to decompose the speed observations. Recall that we refer to this approach as ESD-S. Algorithms are evaluated in terms of detection and false alarm rates. We set the chunk size to ten in both schemes. The results shown in Table V are computed by taking the average of the false alarm and detection accuracy obtained at different vehicles in the platoon.

It is observed that the proposed GESD-physics approach achieves a superior performance in terms of detection accuracy and false alarm rate compared to ESD-S. Fig. 6 shows the false alarm rate, accuracy, and recall for the two mechanisms when applied at each vehicle. We also evaluate the performance using different chunk sizes $C_w = 5$ and 20. Results are shown for each vehicle in Fig. 7. It can be observed that the detection accuracy improves as the chunk size increases from ten to twenty and degrades when the chunk size decreases to five.



(a) ESD-S



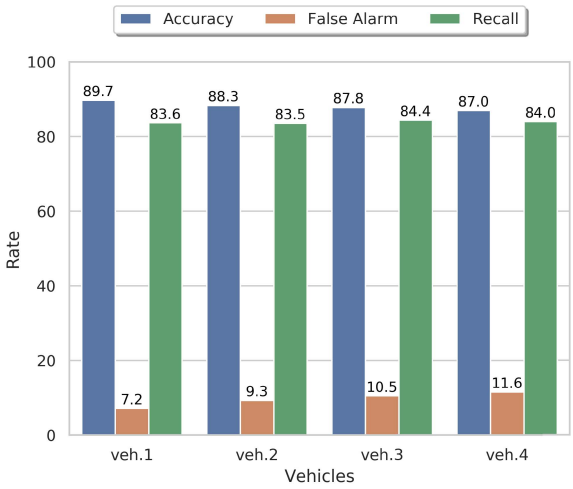
(b) GESD-physics

Fig. 6. Confusion matrix of (a) the ESD-S approach and (b) our proposed mechanism.

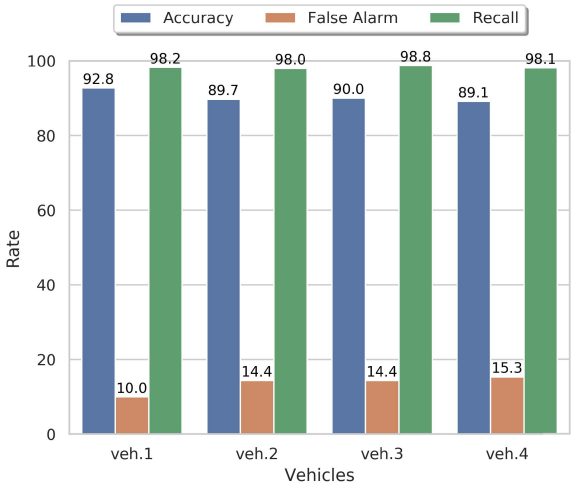
This is expected, since more data improves the accuracy of the statistical GESD; however, the processing time increases as chunk size increases.

C. Time Performance

We evaluate the processing time of the proposed scheme and compare it with the existing ESD-S method in [24]. The processing time is an important metric in CACC. According to [32], packets should be broadcasted by the platoon leading vehicle at most every 100ms for lower risk of collision and faster platooning. The execution times of the proposed scheme and the ESD-S are shown in Fig. 8 for different chunk sizes. As can be seen, our proposed mechanism requires a shorter processing time, and is able to produce the detection results in less than 10ms. Also, when the chunk size increases to 60 observations, our mechanism still produces the detection outcomes before the arrival of the leader's new acceleration value (within 100ms). On the other hand, ESD-S approach fails to provide results within 100ms regardless of the chunk size,



(a) $C_w = 5$



(b) $C_w = 20$

Fig. 7. Our proposed scheme performance at each following vehicle in the platoon using different chunk sizes.

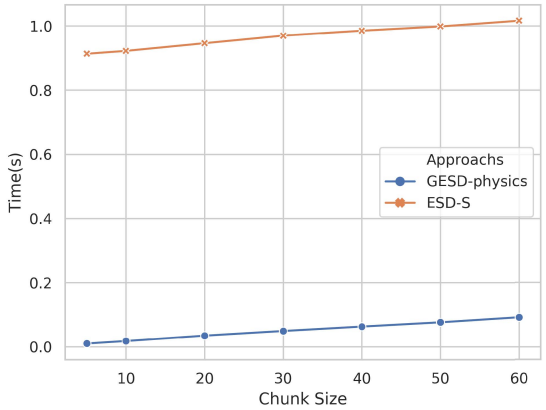


Fig. 8. Processing time of each anomaly detection mechanism under different chunk sizes. Processing time is based on the core computation of the detection algorithms including the wait time needed for obtaining the speeding observations (chunk), but discarding any preprocessing or communications time.

which implies that platoon members would get new messages from the leader before completing the computation of the anomaly detection.

VII. Conclusion

In this paper, we focused on anomaly detection in CACC, which is one of the promising cooperative driving applications in autonomous vehicles. The operation of CACC heavily relies on the reliability of a leader vehicle. We considered one of the serious security threats in CACC, in which a platoon leader is compromised and broadcasts false acceleration information to platoon members. We measured the impact of the attack on road utilization efficiency, passenger comfort, and road safety. To detect the falsification attack, we first proposed to apply information sharing in the CACC model, where information about a leader is collaboratively sensed by the infrastructure and neighboring vehicles, and shared with platoon members. Then, we proposed real-time anomaly detection mechanisms to detect falsification attacks at each platoon member. To detect anomalies in real-time, we proposed GESD-SC approach, which is applied at each vehicle on sliding chunks of the vehicle's own speeding decisions. In addition, by imposing the physics laws of kinematics, we detect suspicious reports of the platoon leader. We proposed a combined approach of GESD-SC and kinematic model to improve the detection accuracy. The combined GESD-SC and physics-based approach has shown to provide an improved detection probability and maintain a low false alarm rate. The combined approach detected more than 92% of the forged data with less than 13% false alarms. Furthermore, we evaluated the execution time performance of the proposed mechanism under different chunk sizes. We highlighted the trade-off between detection accuracy and latency, as we vary the chunk size. It was shown that the computation time of the combined detection approach is within the acceptable range for a platoon operation (less than 100ms). Overall, we conclude that for efficient and high-confidence operation, autonomous vehicles must examine possible anomalies in information relied on for autonomous decisions; learning and modeling the dynamics of the physical system can substantially improve the effectiveness of this task. Further research is needed to study different attack scenarios and mobility models, as well as the impact of communications failures, errors and delays in information sharing.

References

[1] *The Future of Smart Cities: Cyber-Physical Infrastructure Risk*, Dept. Homeland Secur., Washington, DC, USA, 2015.

[2] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," in *Proc. DEFCON*, 2016, pp. 1–70.

[3] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Sep. 2014.

[4] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 993–1006, Sep. 2014.

[5] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR," in *Proc. Black Hat Eur.*, Nov. 2015, pp. 1–13.

[6] Tesla. (Mar. 2016). *A Tragic Loss*. [Online]. Available: https://www.tesla.com/blog/tragic-loss

[7] L. Kong, M. K. Khan, F. Wu, G. Chen, and P. Zeng, "Millimeter-wave wireless communications for IoT-cloud supported autonomous vehicles: Overview, design, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 62–68, Jan. 2017.

[8] K. Dar, M. Bakhouya, J. Gaber, M. Wack, and P. Lorenz, "Wireless communication technologies for ITS applications," *IEEE Commun. Mag.*, vol. 48, no. 5, pp. 156–162, May 2010.

[9] N. Kumar, A.-S. K. Pathan, E. P. Duarte, and R. A. Shaikh, "Critical applications in vehicular ad hoc/sensor networks," *Telecommun. Syst.*, vol. 58, no. 4, pp. 275–277, 2015.

[10] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 289–299, Aug. 2014.

[11] J. Zhao, T. Arnold, Y. Zhang, and G. Cao, "Extending drive-thru data access by vehicle-to-vehicle relay," in *Proc. 5th ACM Int. Workshop Veh. Inter-NETw. (VANET)*, ACM, 2008, pp. 66–75.

[12] L. Hobert, A. Festag, I. Llatser, L. Altomare, F. Visintainer, and A. Kovacs, "Enhancements of V2X communication in support of cooperative autonomous driving," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 64–70, Dec. 2015.

[13] A. Eskandarian, *Handbook of Intelligent Vehicles*, vol. 2. London, U.K.: Springer, 2012.

[14] NHTSA. (2014). *USDOT to Move Forward With Vehicle-to-Vehicle Communication Technology for Light Vehicles*. [Online]. Available: https://www.transportation.gov/briefing-room/us-department-transportation-announces-decision-move-forward-vehicle

[15] L. Guvenc *et al.*, "Cooperative adaptive cruise control implementation of team Mekar at the grand cooperative driving challenge," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 3, pp. 1062–1074, Sep. 2012.

[16] M. Faezipour, M. Nourani, A. Saeed, and S. Addepalli, "Progress and challenges in intelligent vehicle area networks," *Commun. ACM*, vol. 55, no. 2, pp. 90–100, Feb. 2012.

[17] J. Jing, A. Kurt, E. Ozatay, J. Michelini, D. Filev, and U. Ozguner, "Vehicle speed prediction in a convoy using V2 V communication," in *Proc. IEEE 18th Int. Conf. Intell. Transp. Syst.*, Sep. 2015, pp. 2861–2868.

[18] B. Park, K. Malakorn, and J. Lee, "Quantifying benefits of cooperative adaptive cruise control toward sustainable transportation system," Center Transp. Stud., Univ. Virginia, Charlottesville, VA, USA, Tech. Rep., May 2011.

[19] M. Amoozadeh *et al.*, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 126–132, Jun. 2015.

[20] M. Kaur, J. Martin, and H. Hu, "Comprehensive view of security practices in vehicular networks," in *Proc. Int. Conf. Connected Vehicles Expo (ICCVE)*, Sep. 2016, pp. 19–26.

[21] D. Ulybyshev, A. Oqab Alsalem, B. Bhargava, S. Savvides, G. Mani, and L. Ben Othmane, "Secure data communication in autonomous V2X systems," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Jul. 2018, pp. 156–163.

[22] T. Weil, "VPKI hits the highway: Secure communication for the connected vehicle program," *IT Prof.*, vol. 19, no. 1, pp. 59–63, Jan. 2017.

[23] B. DeBruhl, S. Weerakkody, B. Sinopoli, and P. Tague, "Is your commute driving you crazy? A study of misbehavior in vehicular platoons," in *Proc. 8th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*. New York, NY, USA: ACM, 2015, p. 22.

[24] S. Ucar, S. C. Ergen, and O. Ozkasap, "Data-driven abnormal behavior detection for autonomous platoon," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Nov. 2017, pp. 69–72.

[25] M. Jagielski, N. Jones, C.-W. Lin, C. Nita-Rotaru, and S. Shiraishi, "Threat detection for collaborative adaptive cruise control in connected cars," in *Proc. 11th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*. New York, NY, USA: ACM, 2018, pp. 184–189.

[26] F. Alotibi and M. Abdelhakim, "Anomaly detection in cooperative adaptive cruise control using physics laws and data fusion," in *Proc. IEEE 90th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2019, pp. 1–7.

[27] M. Amoozadeh, H. Deng, C.-N. Chuah, H. M. Zhang, and D. Ghosal, "Platoon management with cooperative adaptive cruise control enabled by VANET," *Veh. Commun.*, vol. 2, no. 2, pp. 110–123, Apr. 2015.

[28] J.-M. Chung, M. Kim, Y.-S. Park, M. Choi, S. Lee, and H. S. Oh, "Time coordinated V2I communications and handover for WAVE networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 545–558, Mar. 2011.

[29] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the united states," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

[30] 5G Automative Association. (Jun. 2019). *Press Releases: 5GAA Brings Together Key Actors to Share Advances on C-V2X Deployment in China at MWC Shanghai 2019*. [Online]. Available: https://5gaa.org/news/5gaa-brings-together-key-actors-to-share-advances-on-c-v2x-deployment-in-china-at-mwc-shanghai-2019/

[31] A. Petrillo, A. Pescapé, and S. Santini, "A collaborative approach for improving the security of vehicular scenarios: The case of platooning," *Comput. Commun.*, vol. 122, pp. 59–75, Jun. 2018.

[32] G. Nardini, A. Virdis, C. Campolo, A. Molinaro, and G. Stea, "Cellular-V2X communications for platooning: Design and evaluation," *Sensors*, vol. 18, no. 5, p. 1527, 2018.

[33] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*, Standard ETSI TS 102 637-2 V1.2.1, 2011.

[34] *Dedicated Short Range Communications (DSRC) Message Set Dictionary*, SAE Standard J2735, Venture Capital Trusts Committee, 2016.

[35] K. Ansari, "Cloud computing on cooperative cars (C4S): An architecture to support navigation-as-a-service," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2018, pp. 794–801.

[36] P. Kachroo, N. Shlayan, S. Roy, and M. Zhang, "High-performance vehicle streams: Communication and control architecture," *IEEE Trans. Veh. Technol.*, vol. 63, no. 8, pp. 3560–3568, Oct. 2014.

[37] A. Ghosh, V. V. Paranthaman, G. Mapp, O. Gemikonakli, and J. Loo, "Enabling seamless V2I communications: Toward developing cooperative automotive applications in VANET systems," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 80–86, Dec. 2015.

[38] S. Chen, J. Hu, Y. Shi, and L. Zhao, "LTE-V: A TD-LTE-based V2X solution for future vehicular network," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 997–1005, Dec. 2016.

[39] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRC and cellular network technologies for V2X communications: A survey," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9457–9470, Dec. 2016.

[40] X. Chen and L. Wang, "A cloud-based trust management framework for vehicular social networks," *IEEE Access*, vol. 5, pp. 2967–2980, 2017.

[41] D. S. Berry and D. M. Belmont, "Distribution of vehicle speeds and travel times," in *Proc. 2nd Berkeley Symp. Math. Statist. Probab.* Oakland, CA, USA: The Regents of the Univ. of California, 1951, pp. 589–602.

[42] NIST. (2015). *Extreme Studentized Deviate Test*. [Online]. Available: https://www.itl.nist.gov/div898/software/dataplot/refman1/auxillar/esd.htm

[43] C. Lei, E. M. van Eenennaam, W. Klein Wolterink, J. Ploeg, G. Karagiannis, and G. Heijenk, "Evaluation of CACC string stability using SUMO, simulink, and OMNeT++," *EURASIP J. Wireless Commun. Netw.*, vol. 2012, no. 1, p. 116, Dec. 2012.

Faris Alotibi received the bachelor's degree in information systems from Taibah University in 2011, and the master's degree in information security from the University of Pittsburgh, in 2017, where he is currently pursuing the Ph.D. degree with the School of Computing and Information. He was a System and Application Developer with RCY from 2011 to 2012 and a Teaching Assistant with Taibah University from 2012 to 2015. He is also a Lecturer with the College of Computer Science and Engineering, Taibah University. His research interests include anomaly detection, security, blockchain, cyber-physical systems, machine learning, and insider threats.

Mai Abdelhakim received the bachelor's and master's degrees in electronics and communications engineering from Cairo University in 2006 and 2009, respectively, and the Ph.D. degree in electrical engineering from Michigan State University in 2014. She was with the Egyptian National Center for Radiation Research and Technology from 2008 to 2010. She was a Post-Doctoral Research Associate with Michigan State University from 2014 to 2015. She was a Post-Doctoral Research Scientist with OSRAM from 2015 to 2016. She was a Visiting Assistant Professor with the School of Computing and Information, University of Pittsburgh. She is currently an Assistant Professor of electrical and computer engineering (ECE) with the University of Pittsburgh. Her research interests include cyber-physical systems, security, machine learning, stochastic systems modeling, and information theory.