sensors

MDPI

*Article*

# RSU-Based Online Intrusion Detection and Mitigation for VANET

**Ammar Haydari † and Yasin Yilmaz ***

Electrical Engineering Department, University of South Florida, Tampa, FL 33620, USA
* Correspondence: yasiny@usf.edu
† Current address: Electrical and Computer Engineering Department, University of California, Davis, CA 95616, USA.

**Abstract:** Secure vehicular communication is a critical factor for secure traffic management. Effective security in intelligent transportation systems (ITS) requires effective and timely intrusion detection systems (IDS). In this paper, we consider false data injection attacks and distributed denial-of-service (DDoS) attacks, especially the stealthy DDoS attacks, targeting integrity and availability, respectively, in vehicular ad-hoc networks (VANET). Novel machine learning techniques for intrusion detection and mitigation based on centralized communications through roadside units (RSU) are proposed for the considered attacks. The performance of the proposed methods is evaluated using a traffic simulator and a real traffic dataset. Comparisons with the state-of-the-art solutions clearly demonstrate the superior detection and localization performance of the proposed methods by 78% in the best case and 27% in the worst case, while achieving the same level of false alarm probability.

**Keywords:** vehicular ad-hoc networks; statistical anomaly detection; machine learning; false data injection attack; DDoS attack; road side unit



**Citation:** Haydari, A.; Yilmaz, Y. RSU-Based Online Intrusion Detection and Mitigation for VANET. *Sensors* **2022**, *22*, 7612. https://doi.org/10.3390/s22197612

Academic Editors: Anastasios Doulamis, Nikolaos Doulamis and Athanasios Voulodimos

Received: 30 August 2022
Accepted: 5 October 2022
Published: 8 October 2022



## 1. Introduction

Improving transportation safety is one of the main research areas for intelligent transportation systems (ITS) [1]. An important facilitator for secure and reliable traffic flow is data dissemination through Vehicular Ad-Hoc Network (VANET), including vehicle-to-vehicle (V2V) communications and vehicle-to-infrastructure (V2I) communications. VANET is a promising technology that enables communications between driverless autonomous vehicles, which are expected to dominate future traffic, as well as traditional vehicles controlled by a driver [2,3]. VANET applications can be classified into two types, traffic safety applications and traffic management applications. Route planning applications for drivers are an example of traffic management applications. The safety-related applications are exemplified by road condition applications and accident information systems.

There are two possible communication methods for VANET: (i) 5.9 GHz dedicated short-range communication (DSRC) and (ii) cellular-based vehicular communication [4]. With fast advancing 5G technologies for connected and automated vehicles, the industry is more inclined to support cellular-based communication technologies, named cellular vehicle to everything (C-V2X) [5]. Recently, Europe and the US both announced to advance their technologies for cellular-based VANET. Although cellular network models are more decentralized, still such C-V2X communication requires RSU or some sort of base station near the roads as an infrastructure component in order to collect and process traffic and vehicular data [6].

In VANET, different types of data, such as position information, road conditions and emergency messages, are disseminated. The availability and integrity of such data are the two essential aspects of VANET security. Distributed roadside units (RSUs) have a critical role in VANET as a static infrastructure over the roads for centralized communication. RSUs provide high connectivity and safety in traffic with periodic and aperiodic message

dissemination. However, VANET communication, especially the centralized RSU unit, is highly vulnerable to cyberattacks. Considering the potential life-threatening outcomes in traffic, cyberattacks on VANET need to be quickly and accurately detected and mitigated.

The security of VANET is extensively studied in the literature [7,8]. However, the main security solutions to the RSU-based VANET communication have a lack of generalization to different data types, attack models, and scenarios. Recent security models in the literature mainly assume specific data structures for false data injection attacks and specific attack strategies for DDoS attacks. To this end, in this paper, we propose a centralized RSU-based anomaly detection and mitigation method for cyberattacks targeting both data availability and integrity without a specific data structure or an attack strategy.

### 1.1. False Data Injection Attacks Targeting Integrity

Falsified message content may cause the drivers to take wrong actions entailing devastating and life-threatening results for vehicular traffic. Autonomous vehicles are exposed to even greater risk due to false data injection (FDI) attacks, as their automatic decisions may rely more on the received VANET messages. For example, the position is one of the most important pieces of information in VANET; when a vehicle sends wrong positional information, then a nearby autonomous vehicle may accelerate according to the received falsified message. An effective intrusion detection system (IDS) should effectively deal with FDI attacks, in which an attacker sends bogus information to the network in order to change the vehicle behavior in traffic. Once an intruder injects bogus data into the network, it should be detected and mitigated timely to prevent a major problem, such as an accident or traffic congestion.

There are several detection approaches for different FDI attack models. Trust-based security mechanisms and behavior-based security mechanisms are two common signature-based detection approaches for FDI attacks in the literature. However, they are mostly not computationally efficient and cannot detect new attack patterns that do not conform to the known signatures [9,10]. In this work, we propose an anomaly detection method that can quickly detect FDI attacks, including previously unseen ones, as opposed to the signature-based methods. Our method is implemented on RSU, and it monitors the data stream received from each vehicle within its communication range. We do not use any revocation list or voting list scheme. Once our method detects an anomalous vehicle, it blocks the data transfer from that vehicle and informs the other vehicles.

### 1.2. DDoS Attacks Targeting Availability

Availability of communications is one of the main objectives of ITS. Denial-of-service (DoS) attacks target the availability of network service, e.g., by sending high volumes (flooding) of data packets to the service provider. Once a DoS attack is launched successfully on VANET, e.g., on RSU, the system operation shuts down such that no one can get regular service. The unavailability of the VANET service due to a DoS attack may cause significant damage to vehicular traffic. Compared to the FDI attack, it is easier to initiate a DoS attack for attackers as no data manipulation is needed; however, the FDI attack poses a bigger threat since wrong data are usually more detrimental than no data. In practice, to make the mitigation more difficult, attackers synchronously launch a DoS attack from multiple sites, which is called a Distributed DoS (DDoS) attack. The proliferation of Internet-of-Things (IoT) devices, in particular autonomous vehicles, facilitates a new type of stealthy DDoS attack, called low-rate DDoS [11,12], which can easily bypass traditional IDSs such as data traffic filters and firewalls while still causing significant disruption in the targeted service due to its highly distributed and synchronous nature.

It is quite challenging to timely detect and mitigate stealthy DDoS attacks compared to the standard brute-force DDoS attacks because the increase in the individual data rates from multiple parties with respect to their nominal baselines can be very low such that traditional data filtering methods cannot detect them. Yet, the aggregate increase in the data traffic received by the targeted RSU from multiple attackers can be tremendous, thus the

RSU gets overwhelmed and stops serving legitimate users. There are three main enabling factors that make such stealthy DDoS attacks relevant in VANET:

*Increasing number of connected vehicles:* In the near future, connected vehicles will be widespread, which will, in turn, increase the attack surface for DDoS attacks. Similar to the Internet of Things (IoT), or as a part of it, this trend is called the Internet of Vehicles (IoV). The growing attack surface will enable effective DDoS attacks to require fewer increases in data rate (i.e., less attack signature) and to be more stealthy in nature over time.

*Public V2I communications:* Since V2I communication is open to everyone, attackers can utilize many other IoT devices that pretend to be vehicles to spoof the RSU. Such non-vehicle attacking devices can be on vehicles or static within the communication range of RSUs. The possibility to use IoT devices for attacking RSU greatly extends the attack surface, making stealthy DDoS a big threat for VANET.

*Sybil attack:* Furthermore, through Sybil attack, the attackers do not even need to utilize many devices (vehicle or non-vehicle) for an effective stealthy attack. In Sybil attack, a single vehicle pretends to be multiple vehicles by creating fake identities. Hence, a single vehicle can transmit a huge amount of data packets to the RSU, appearing as coming from different vehicles at low transmission rates. This efficient attack strategy can generate stealthy DDoS attacks by using only a fraction of the number of vehicles/devices that are normally needed.

In this paper, we propose a powerful multivariate method for the timely detection and mitigation of stealthy DDoS attacks on RSU.

### 1.3. Contributions

In this paper, we propose a novel anomaly-based detection and mitigation technique to address FDI attacks and flooding-based (stealthy or brute-force) DDoS attacks targeting VANET, in particular RSU. Our contributions can be summarized as follows.

- A novel machine learning detector for RSU is proposed for FDI and DDoS attacks.
- The asymptotic false alarm rate of the proposed detector is analyzed, and a closed-form expression for the detection threshold is derived based on this analysis.
- Based on the detection method, an anomaly localization and accordingly attack mitigation method is proposed for FDI and DDoS attacks for VANET.
- Performance of the proposed detection and mitigation methods are extensively evaluated using state-of-the-art traffic simulators and a real traffic dataset. To the best of our knowledge, this is the first work to use real traffic data in the cybersecurity literature for VANET.

The rest of the paper is organized as follows. Related works are discussed in Section 2. The traffic and attack models for the considered attack types are given in Section 3. The proposed anomaly detection and mitigation methods are presented in Section 4. Numerical results are provided in Section 5. Finally, the paper is concluded in Section 6. Throughout the paper, lowercase and uppercase bold letters are used to denote vectors and matrices, respectively.

## 2. Related Work

### 2.1. False Data Injection Attacks

The injection of fake messages is a high threat to ITS/VANET security [13]. Several key features differentiate VANET and ITS security from other network security topics, such as high mobility, dynamic characteristics, and life-threatening conditions. One popular type of FDI attack is misbehavior detection, where data are compared with the behavior of vehicles. Many misbehavior detection models for VANET are proposed in the literature, considering either the trust-centric or data-centric strategy for enhancing the security of VANETs [14–16]. However, these models mostly rely on the data content, which makes them not generalizable. Trust-centric models are based on voting or scoring schemes in which the reliability of a node broadcasting a message is voted on by the other nodes receiving the message. Once the cumulative voting score exceeds a level against the node, it

is declared as an intruder, and its message dissemination is blocked [17–19]. A data-centric approach evaluates the driver's behavior with respect to shared messages. In [20], an example data-centric detection model is proposed for emergency messages.

There are several misbehavior detection mechanisms for VANET based on statistical and machine learning (ML) approaches. Authors in [21] proposed a decentralized misbehavior detection mechanism using a context-reference model with Kalman and Hample filters to extract the consistency of messages with the behavior of vehicles. A statistical misbehavior detection model using entropy-based classification is proposed in [22]. The authors of [23] proposed a trust-based misbehavior detection model integrated with entropy modeling and reinforcement learning. In [24,25], intrusion detection mechanisms are proposed against multiple attack types, including FDI and packet drop attacks, using vehicle reputation scores collected by RSUs. In [26], the authors proposed a statistical anomaly detection technique considering only the data content instead of the trust score or revocation list to detect anomalous nodes that inject falsified data into VANET. This paper uses the Greenshield traffic model assuming close vehicles have similar flow, speed, and density values. In decentralized traffic, each vehicle calculates its value and compares it with average received values until the average value is below the predefined threshold. After that, a t-test is applied to these values to determine if the received message comes from an intruder or not. Recently, a new security mechanism for VANET has been proposed in [27] with a novel detection and classification mechanism using a hidden generalized mixture transition distribution model. In this work, the detector collects the data of each vehicle in feature tables, and the classifier processes the extracted knowledge.

Anomaly detection mechanisms based on ML provide suitable results for security mechanisms in general. Recently, several ML-based IDS models have been studied for ITS/VANET [28–30]. In [28,31], the authors study a trust-based cyberattack detection model for false position, timing, and Sybil attacks. A security model based on a plausibility check is studied using ML in [29], where the authors considered supervised *k*NN and SVM algorithms for detecting anomalies on feature vectors by experimenting with the VaReMi dataset [32]. An improved version of this work, by introducing new plausibility check methods, is presented in [33]. Although this is not a centralized detection model, it still requires some information from RSU or a trustworthy source for calculating the plausibility feature vector. A cooperative misbehavior detection model is proposed in [30] for detecting emergency message and position falsification attacks. In [34–36], the authors studied supervised learning models for detecting false position attacks in VANET. A new research direction studies false data injection attacks using time-series ML models, such as LSTM or GRU [37,38].

### 2.2. Denial-of-Service Attacks

DoS attacks may cause catastrophic effects on vehicular traffic since the decisions of vehicles may critically depend on the communications between the vehicles and the infrastructure [39]. There are several solution methods proposed for DoS attacks in the literature. Early studies mainly target the DoS attacks considering a single attack source [40,41]. A packet delivery ratio-based jamming attack detection model for VANET was presented in [42] for two traffic scenarios. However, these methods are not suitable for detecting stealthy DDoS attacks as they directly compare the observed packet rate to a threshold.

Several trust-based defense mechanisms for DDoS attacks in VANET [43–45] rely on the trust score of neighboring vehicles. These studies propose fixed and learning-based trust mechanisms for different VANET scenarios. An unsupervised detection method based on the k-means clustering algorithm was proposed in [46] for jamming attacks in RF-based vehicular communication. Another work [47] on jamming attacks for platooning vehicles in VANET studies a hybrid detection model with a statistical approach. This detection model focuses only on platooning vehicles to detect jamming attacks and does not apply to other DDoS attacks. The authors of [48] proposed a DDoS detection model for VANET, where they use a multivariant stream analysis (MVSA) approach. Since this IDS follows a window-

based approach, the size of time windows limits its timely detection performance. Recently, many supervised ML models have been studied for different DDoS attack models for VANET [49–52]. In [53], we proposed an anomaly-based IDS for mitigating DDoS attacks in VANET, which is significantly enhanced with theoretical and experimental results, and extended to FDI attacks in this paper.

There are some other security mechanisms proposed for other attack types. Black hole attack or packet drop attack, in which packets are deliberately dropped at a compromised node, is another type of DoS attack studied in the VANET literature. For instance, Ref. [54] proposed an SVM-based detection method for clustered VANET. In Sybil attack, an attacker identifies itself as multiple nodes. For example, in [55], the authors considered detecting Sybil attacks using strength analysis for received signals with statistical position verification.

### 2.3. Comparisons

Our work has several novelties compared to the existing methods in the literature. First, the existing IDS models consider several attack strategies that only target one security objective, e.g., IDS, for data integrity. Our proposed security model addresses two distinct attack types, FDI and DDoS.

Regarding the FDI attacks, the studies discussed up to now consider network-level IDSs, which are not suitable for detecting collaborative FDI attacks with multiple attackers. Our proposed anomaly-based IDS at RSU classifies each vehicle as malicious or benign, and it is robust to collaborative FDI attacks. Once detected, such an attack is easily mitigated by dropping packets from attackers without interrupting benign communications. Since our proposed model is a statistical IDS, it is not restricted to any message format and data content. After it detects the FDI attack, it also identifies the specific data type under attack, such as speed, position, or emergency message.

Regrading the DDoS attack, our proposed method is advantageous compared to the existing works in several ways: (i) it does not consider any specific data model for DDoS attacks, (ii) it successfully detects highly distributed DoS attacks from many attackers, and (iii) it can handle both stealthy and traditional brute-force DDoS attacks. In stealthy DDoS, as demonstrated recently on the Internet [56], while slightly increasing the data rate from one source does not affect the regular performance of the receiver node, attacking from multiple sources, even with slightly increasing the transmitted data rate, can cumulatively overwhelm the receiver node.

Recent ML-based methods are based on sample-by-sample outlier detection and do not continuously update their statistics for detecting anomalies, as opposed to our proposed sequential detection method. The sample-by-sample outlier detection approach is prone to frequent false alarms due to nominal outliers [57], while sequential methods can avoid nominal outliers and detect only the persistent outliers as anomalous [58].

## 3. System Model

### 3.1. VANET Model

A general two-way traffic flow is considered, as shown in Figure 1. However, the proposed IDSs are not restricted to a specific road type; they can perform well in different scenarios such as one-way traffic, two-way traffic, urban area, highway area etc. Vehicle-to-vehicle (V2V) and vehicle-to-RSU (V2I) communications based on broadcasting take place in the considered VANET model to disseminate beacon messages. In general, such messages may have various content. In this work, we consider that each vehicle regularly broadcasts messages in the (ID, speed, position, direction) format.

All messages are protected with cryptographic algorithms, but such details are out of the scope of this paper. We assume that different pseudonyms are assigned by a central authority to each vehicle for providing authenticity and identification. Thus, the ID of each vehicle is always known by the RSUs. Collected messages can be used for different purposes, but they are mostly used for informing other vehicles on the road. For instance, an RSU calculates the average speed and the density of the road using the received beacon

messages from the vehicles in its range, and conveys these calculated messages to the other RSUs to inform the vehicles that are not in range. RSUs play a central role in the security of VANET. Hence, we propose a statistical IDS that runs at each RSU. Although the beacon messages are already encrypted for secure communications, the integrity, i.e., correctness, of message content, as well as the availability of VANET communications, should be maintained.

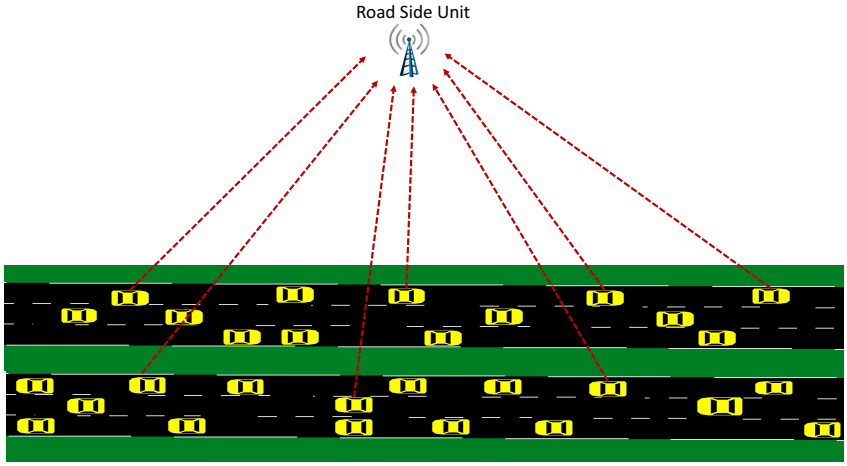


**Figure 1.** Traffic model for the nominal case where all vehicles broadcast messages and RSU collects these messages.

### *3.2. Attack Model*

In this work, we consider two types of attacks in VANET.

#### 3.2.1. False Data Injection Attacks

Creating a completely false message or changing some parameters of a message may have a crucial impact on the traffic. Although today's traffic is not yet dominated by fully autonomous vehicles, in the near future, it is expected that the majority of vehicles will decide by themselves without human interaction. In such a scenario, disseminating correct messages to other vehicles is a top priority for VANET. For example, a malicious vehicle conveying false messages about its position and speed may cause other vehicles to take wrong actions, such as decreasing speed or changing lanes. Even without any malicious intent, faulty sensors in a vehicle may result in false messages. The proposed RSU-based statistical IDS can quickly detect FDI attacks and accurately identify the false data type and its source vehicle.

#### 3.2.2. Distributed Denial-of-Service Attacks

In the considered DDoS attack, the number of messages per unit time, i.e., data rate, such as packets/sec., from multiple sources (vehicles or other devices pretending to be vehicles) increases synchronously (No strict synchronization is needed to perform a DDoS attack). Unless quickly detected and mitigated, such flooding of messages may easily overwhelm the attacked RSUs to make the VANET communications unavailable. It is significantly more challenging to detect and mitigate stealthy DDoS attacks than traditional brute-force DDoS attacks. The aggregate data rate received by the RSU is still high enough to take it down; however, the increase in individual data rates of attacking nodes is low such that they easily remain undetected by traditional IDS, such as data filters and firewalls. Despite its relatively small increase in individual data rates, the greatness in the number of attacking nodes is what makes a stealthy DDoS attack threatening.

The proposed statistical IDS monitors the data rate. Thus, it is not restricted to the data format defined above. In the following sections, we show that the proposed IDS can

effectively handle both stealthy and brute-force DDoS attacks, as opposed to traditional data filtering methods.

## 4. Proposed Intrusion Detection and Mitigation Systems

In general, anomaly-basedbased IDS works by comparing the observed data instances with the statistical model of nominal operation learned from training data and possibly also with the anomalous statistical model learned from training data as well. Anomaly-based IDS can be categorized considering three aspects: availability of training data, parameterization of statistical model, and sequential decision making.

In terms of the availability of training data, anomaly-based IDS can be categorized into groups, semi-supervised and supervised. If there is only nominal training data, IDS aims to detect significant deviations from the learned nominal statistical model, which is called the semi-supervised setting. Whereas, in the supervised setting, IDS also builds a statistical model for the considered attacks using available data instances from previous attack cases and compares the goodness-of-fit (e.g., likelihood) of the observed data under the nominal and attack models.

In terms of model parameterization, there are also two types, parametric and non-parametric methods. While parametric methods try to fit certain parametric probability distributions (e.g., Gaussian, Poisson, etc.) to the data, non-parametric methods try to learn statistical patterns from the data without assuming certain probability distributions (e.g., distance-based and histogram-based methods).

Finally, in terms of sequential decision-making, we also have two groups: sample-by-sample outlier detection methods and sequential anomaly detection methods. Outlier detection methods decide for each observed data instance as either nominal or anomalous. However, sequential methods update a decision statistic using each observed data instance and decide when there is enough statistical evidence for an anomaly. Mathematically, the objective of sequential methods is to minimize the expected number of data instances used to detect anomalies while satisfying a constraint on false alarm rate.

### *4.1. Challenges in VANET for an IDS*

Implementing an anomaly-based IDS in VANET is a challenging task due to several reasons. Three major challenges in VANET for an IDS can be summarized as follows.

(C1) *Unknown attack patterns:* As opposed to the traditional computer networks and the Internet, the possible attack patterns (i.e., signatures) are mostly unknown in the emerging field of ITS/VANET security. Hence, conventional signature-based IDS, which can only detect the known attack signatures, and supervised anomaly-based IDS are, in general, not suitable for VANET.

(C2) *Disparate data types:* Since anomalies occur relative to the context defined by the entire data dimensions, they should ideally be jointly monitored through multivariate analysis. However, due to the disparate data types conveyed in messages, the multivariate probability distribution of the message content is quite complicated. For instance, speed data are numerical, direction is angular, and position is numerical/angular. As a result, parametric anomaly detection methods, which try to fit tractable probability distributions to the training data, are not feasible here.

(C3) *Timely and minimally invasive mitigation:* Considering the life-threatening and economic concerns of a failure in VANET communications, cyberattacks should be quickly mitigated in a minimally invasive manner. The identification of malicious users should also be accurate such that legitimate users continue receiving regular service. It is known that sequential methods are much more effective in timely detection than sample-by-sample outlier detection methods [59].

To address the challenges above, we propose a statistical IDS based on a semi-supervised, non-parametric, and sequential anomaly detection technique.

*4.2. Proposed Detection and Mitigation Method for FDI attack*

In this section, we explain the proposed intrusion detection and mitigation method for FDI attacks. The proposed method is an online intrusion detection system and can work in real-time, similar to a sequential anomaly detection algorithm [60]. Thanks to its semi-supervised, non-parametric, and sequential methodology, the proposed method addresses the challenges (C1)–(C3) well in Section 4.1, respectively.

In the proposed IDS, each RSU runs a separate detector for each vehicle that it receives messages from. In particular, an RSU starts to monitor a vehicle when the vehicle enters its range until either the vehicle exits the range or an anomaly in the message content is detected.

Consider that each data instance $\boldsymbol{x}_i \in \mathbb{R}^d$ is a $d$-dimensional real-valued vector representing the observed $d$ data dimensions $\{x_i^1, \ldots, x_i^d\}$ depending on the application. While we consider (ID, speed, position, direction) as the data dimensions, the proposed detection and mitigation methods are not restricted to this particular setup. The data instances are inspected by an infrastructure unit (RSU) in a centralized fashion for detecting falsified data attacks. We do not have any assumption on the probability distributions of data dimensions, e.g., they can be correlated or even follow disparate distributions. It is only assumed that each data dimension can be normalized to [0, 1] by using the minimum and maximum values, which is needed to deal with the heterogeneity among data dimensions.

In the training phase, first the nominal training data $\mathcal{X}_N = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N\}$ are randomly partitioned into two sets, $\mathcal{X}_{N_1}$ and $\mathcal{X}_{N_2}$, where $N_1 + N_2 = N$, for computational and theoretical purposes. Typically, $N_2$ is selected greater than $N_1$ as explained in Theorem 1. The nominal training data $\mathcal{X}_N$ is obtained through historical observations in the range of RSU. Then, for each data point in $\mathcal{X}_{N_1}$, $k$ nearest neighbors ($k$NN) in $\mathcal{X}_{N_2}$ in terms of Euclidean distance are found. For each point $i$ in $\mathcal{X}_{N_1}$ the total distance $L_i$ is computed as

$$L_i = \sum_{j=k-s+1}^{k} e_{ij}^{\gamma}, \tag{1}$$

where $e_{ij}$ is the Euclidean distance from point $i$ in $\mathcal{X}_{N_1}$ to its $j$th nearest neighbor in $\mathcal{X}_{N_2}$. The weight $\gamma > 0$ and the number of considered neighbors $s$, which is a number between 1 and $k$, are introduced to increase the flexibility of the method.

Next, for a significance level $\alpha$, for which a typical choice is 0.05, the $(1-\alpha)$th percentile $L_{(M)}$ of $\{L_i : i = 1, \ldots, N_1\}$ values are found, where $M = \lfloor N_1(1-\alpha) \rfloor$, and $\lfloor \cdot \rfloor$ is the floor operator. The $L_{(M)}$ value is later used as a baseline in the test to evaluate the anomaly evidence in the test instances. Depending on the VANET structure, if the range of RSU is composed of heterogeneous road segments with different speed and direction baselines, then multiple training sets and, accordingly, multiple $L_{(M)}$ values can be obtained for such road segments. During the training phase, an Euclidean $k$NN graph is actually formed between $(1-\alpha)$% of the points in $\mathcal{X}_{N_1}$ with the smallest $L_i$ values and their neighbors in $\mathcal{X}_{N_2}$, as illustrated in Figure 2. As we will show next, in the test phase, we actually evaluate how far/close a test instance is in becoming a vertex in this graph if it were to be included in $\mathcal{X}_{N_1}$. From another perspective, $(1-\alpha)$% of the points with the smallest $L_i$ values in $\mathcal{X}_{N_1}$ is an estimate of the "minimum volume set" which is the most compact set that has at least $1-\alpha$ probability [61], and in the test phase, we measure how far/close a test instance is to be included in this most compact set.

In the test phase, to evaluate the anomaly evidence in a newly observed instance $\boldsymbol{x}_t$ at time $t$, we compute how small/big the total distance $L_t$ of $\boldsymbol{x}_t$ compared to the baseline $L_{(M)}$, which corresponds to a boundary point in the most compact set of nominal points. Specifically, at each time $t$, we compute the total distance $L_t$ with respect to the nominal training set $\mathcal{X}_{N_2}$, as in (1), and the anomaly evidence

$$D_t = (L_t)^d - (L_{(M)})^d. \tag{2}$$

Note that the anomaly evidence provided by $D_t$ can be positive or negative. Unlike the sample-by-sample outlier detection methods, the proposed IDS does not decide for each instance but rather accumulates the anomaly evidence over time by updating its decision statistic as

$$s_t = \max\{s_{t-1} + D_t, 0\},\ s_0 = 0. \tag{3}$$

It decides for an anomaly only when enough evidence is accumulated in the decision statistic, i.e., at time

$$T = \min\{t : s_t \geq h\}, \tag{4}$$

similar to the CUSUM algorithm [58]. Note that the proposed IDS in (1)–(4) is a novel data-driven algorithm, as opposed to the parametric (model-based) CUSUM algorithm.

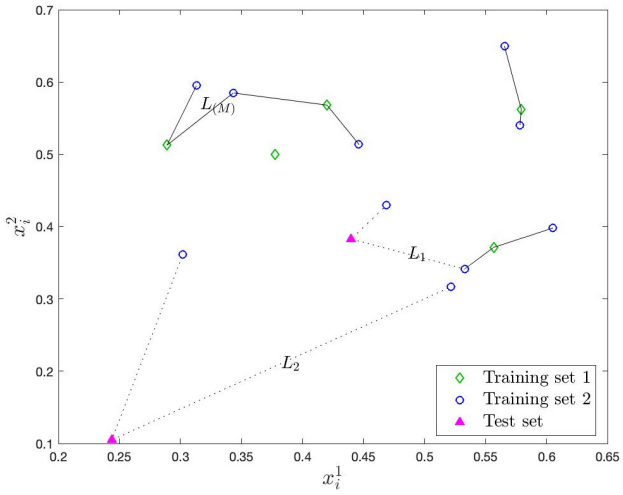


**Figure 2.** Proposed detection procedure with $N_1 = 5$, $N_2 = 10$, $M = 4$, $k = 2$, $s = 1$, $\gamma = 1$. $(L_1)^d - (L_{(M)})^d$ and $(L_2)^d - (L_{(M)})^d$ are used to update the test statistic $s_t$ and raise athen alarm at time $T$, as shown in (1)–(4). Training and test points are generated from a bivariate normal distribution with independent components, 0.5 mean and 0.1 standard deviation.

The detection threshold $h$ manifests a trade-off between minimizing the detection delay and the false alarm rate. For example, higher $h$ decreases the false alarm rate at the expense of a larger average detection delay, and vice versa for lower $h$. Next, we show how to set $h$ to satisfy a desired false alarm rate.

**Theorem 1.** *As the training set grows ($N_2 \to \infty$), with $k = s = \gamma = 1$, to asymptotically ensure that the false alarm rate is less than or equal to the desired level $\beta$, the threshold $h$ can be chosen as follows*

$$h = \frac{-\log \beta}{\omega_0}. \tag{5}$$

*In (5), $\omega_0 > 0$ is given by*

$$\omega_0 = v_d - \theta - \frac{1}{\phi}\mathcal{W}\left(-\phi\theta e^{-\phi\theta}\right),$$
$$\theta = \frac{v_d}{e^{v_d L_{(M)}^d}},$$

*where $\mathcal{W}(\cdot)$ is the Lambert-W function, $v_d = \frac{\pi^{d/2}}{\Gamma(d/2+1)}$ is the constant for the d-dimensional Lebesgue measure (i.e., $v_d L_{(M)}^d$ is the d-dimensional volume of the hyperball with radius $L_{(M)}$), and $\phi$ is the upper bound for $D_t$.*

**Proof.** See Appendix A. □

Although the expression for $h$ looks complicated, all the terms in (5) can be easily computed. Particularly, $v_d$ is directly given by the dimensionality $d$, $L_{(M)}$ comes from the training phase, $\phi$ is also found in training, and finally, there is a built-in Lambert-W function in popular programming languages, such as Python and Matlab. Hence, given the training data, $\omega_0$ can be easily computed, and based on Theorem 1, threshold $h$ can be chosen to asymptotically achieve the desired false alarm rate.

In the non-asymptotic practical region, where the number of training instances, $N_2$, is finite, the threshold $h$ can still be approximately set using (5). The quality of this approximation depends on the amount of training data. With more training data, (5) will be a better approximation. Further, with more training data, a smaller threshold can be used to achieve the desired false alarm rate $\beta$ as $L_{(M)}, \phi, \theta$ will shrink and, in turn, $\omega_0$ will grow. A smaller threshold means a smaller detection delay. Hence more training data increases the performance of the proposed IDS, as expected. If the desired levels of the average detection delay and false alarm rate cannot be achieved with the current training set, it indicates a need for more training data. The proposed IDS uses training data to discover nominal data patterns; thus, for urban roads with complex patterns, typically more training data are needed compared to a suburban road with simple patterns.

The selection of other parameters also indirectly affects this fundamental trade-off of quick and accurate detection. Particularly, for a bigger/smaller number of neighbors $k$, the proposed IDS becomes more/less robust to noise (i.e., nominal outliers) but at the same time less/more sensitive to anomalies. In turn, bigger/smaller $k$ result in lower/higher false alarm rate and longer/shorter average detection delay. The parameter $s$ is auxiliary to $k$, and yields similar effects in the algorithm. The significance level $\alpha$ does not play a central role, as opposed to the outlier detection methods, in which $\alpha$ directly controls the essential trade-off between the detection probability (i.e., true positive rate) and false alarm probability (i.e., false positive rate). In the proposed IDS, the effect of the $\alpha$ choice can be compensated by the decision threshold $h$, which is the ultimate parameter that directly controls the balance in detection performance. Hence, in practice, first, a typical value, such as 0.05, is selected for $\alpha$, and then $h$ is chosen to satisfy a desired false alarm rate, as shown in Theorem 1.

Detecting an attack is, in general, not the final task for successful mitigation. Each message from vehicles needs to be analyzed for general traffic management systems. A powerful IDS should not ignore the data traffic from anomalous vehicles as a whole; it should identify the anomalous data dimension as soon as possible in order to not allow the attacker to deteriorate the decisions of the control center for specific message dimensions. For instance, the attacker may only report the wrong speed information and the other data contents, e.g., direction and position may still be valuable for RSU. Another motivation for an in-depth mitigation strategy is to inform other RSUs about what data content is under attack so that they can be prepared beforehand. Without a mitigation strategy, after the detection, RSU will not only disregard the entire data traffic from anomalous vehicles but also will not know what specific content of the messages is under attack. To this end, we next propose a statistical anomaly localization technique for the proposed IDS to identify the anomalous data dimensions where an attacker injects falsified data.

In (4), detection occurs due to an increase in the decision statistic $s_t$, given by (3), which is caused by recent positive anomaly evidence(s) $D_t$, given by (2). Moreover, positive $D_t$ happens due to the total distance $L_t$ being greater than the baseline $L_{(M)}$. From (1), we know that $L_t$ is the sum of $s$ Euclidean distances of data instance $\boldsymbol{x}_t$ to its $\{k-s+1, \ldots, k\}$th nearest neighbors. Since, for $\gamma = 2$, each Euclidean distance to a neighbor is the sum of squared distances in the $d$ data dimensions, $L_t$ can be written in the following alternative form

$$L_t = \sum_{n=1}^{d} \ell_t^n \text{ where } \ell_t^n = \sum_{j=k-s+1}^{k} (x_t^n - y_j^n)^2, \tag{6}$$

and $x_t^n$ and $y_j^n$ are the $n$th dimensions of the data instance $\boldsymbol{x}_t$ and its $j$th nearest neighbor $\boldsymbol{y}_j$. Note that $\ell_t^n$ denotes the contribution of dimension $n$ to the total distance $L_t$. Thus, after detection, we can investigate each dimension's contribution to the attack alarm by analyzing some recent $\ell_t^n$ right before the detection time $T$. We determine the number of recent $\ell_t^n$ values contributing to the alarm by first identifying the last time instance $q = \max\{t < T : s_t = 0\}$ when the decision statistic $s_t$ was zero and then started increasing, which can be seen as an estimate for the attack onset time. Then, the average contribution from each dimension $n$ to the attack alarm is computed as

$$\bar{\ell}^n = (T-q)^{-1} \sum_{t=q+1}^{T} \ell_t^n, \tag{7}$$

where $T$ is the detection time, given by (4). Finally, each dimension $n$ is identified as attacking if its average contribution is sufficiently high, i.e., $\bar{\ell}^n \geq \lambda$. The threshold $\lambda$ controls the trade-off between false positive and true positive rates. It is typically selected to satisfy a constraint on the false positive rate [62].

The proposed attack detection and localization technique is summarized in Algorithm 1.

**Algorithm 1** Proposed detection and localization algorithm

*Inititalization*: $s_0 \leftarrow 0$, $t \leftarrow 0$
*Training phase:*
Partition training set $\mathcal{X}_N$ into $\mathcal{X}_{N_1}$ and $\mathcal{X}_{N_2}$
Compute $L_i$ for each $\boldsymbol{x}_i \, \epsilon \, \mathcal{X}_{N_1}$ as in (1)
Find $L_{(M)}$ by selecting the $M$th smallest $L_i$
*Test phase:*
**while** $s_t < h$ **do**
  $t \leftarrow t+1$
  Get new data $\boldsymbol{x}_t$ and compute $D_t = (L_t)^d - (L_{(M)})^d$
  $s_t = \max\{s_{t-1} + D_t, 0\}$
**end while**
Attack detected at time $T = t$
Estimate attack start time as $q = \max\{t < T : s_t = 0\}$
**for** $n = 1, \ldots, d$ **do**
  Compute $\bar{\ell}^n$ as in (7)
  **if** $\bar{\ell}^n \geq \lambda$ **then**
    Declare dimension $n$ as under attack
  **end if**
**end for**

### *4.3. Proposed Detection and Mitigation Method for DDoS*

A straightforward approach to DDoS detection is by comparing the incoming message rate (i.e., the number of messages per unit time) from each vehicle with a threshold. Although this method can stop brute-force attacks in which attackers transmit a burst of data messages at a high rate, it would not be effective against stealthy DDoS attacks in which multiple attackers transmit messages at a slightly-higher-than-nominal rate synchronously, yet together they overwhelm the RSU. Admittedly, the straightforward approach that compares the total data rate from all vehicles with a threshold can easily detect any DDoS attack (either brute-force or stealthy); however, it cannot identify the attackers to stop the attack.

We propose a multivariate statistical IDS that jointly monitor vehicles using Algorithm 1 for detecting and mitigating both stealthy and brute-force DDoS attacks. While univariate methods will fail to detect the malicious vehicles' close-to-nominal data rates in stealthy DDoS, our proposed multivariate approach can easily detect them as simultaneous small increases from multiple vehicles cause a considerable increase in $k$NN distance with respect to the nominal training data.

Since the number of vehicles in the range of an RSU varies over time, for joint monitoring of data traffic, we consider total message rates in a number of predetermined road segments as the input data to the proposed algorithm, $\boldsymbol{x}_t = [x_t^1, \ldots, x_t^d]$, where $x_t^n$ is the message rate from road segment $n$ at time interval $t$. (see Figure 3). Detecting DDoS attacks is not the only goal of an effective IDS; it should also mitigate the detected attack to protect the VANET. Especially for stealthy DDoS attacks, identifying the attacking nodes is a challenging task that must follow detection. Otherwise, after the detection, RSU will either disregard the entire data traffic or wait with no further action until the excessive incoming data paralyzes it. In either case, the DDoS attack would be successful in making the RSU service unavailable. Our proposed attack mitigation strategy will be activated after a DDoS attack is detected to identify the anomalous road segment whose data will be blocked. Since the proposed algorithm is sequential in nature, it can dynamically detect and mitigate DDoS attacks due to moving vehicles in real-time. The proposed IDS for mitigating DDoS attacks is summarized in Figure 4.

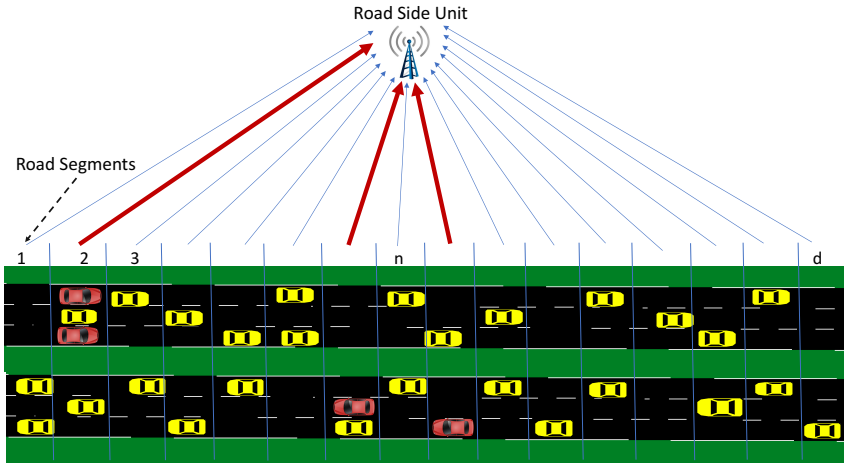


**Figure 3.** DDoS attack model where red cars are attackers and thick red lines denote the increased data rates.

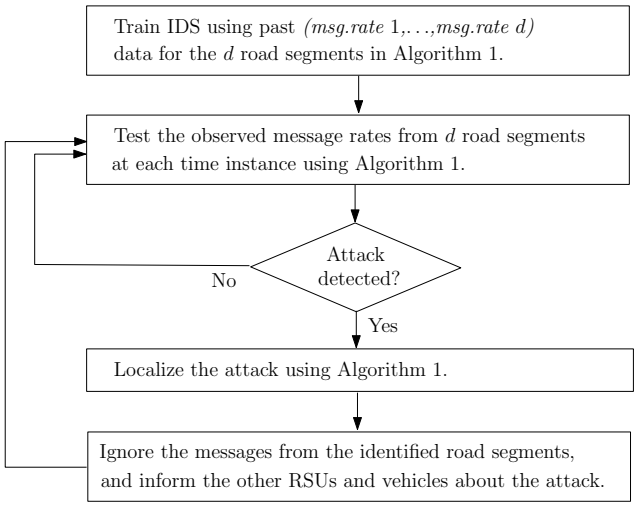


**Figure 4.** Flowchart of the proposed IDS for DDoS attacks.

### *4.4. Computational Complexity*

This section analyzes the computational complexity of the proposed sequential anomaly detection module. In the training phase, computing $L_M$, $k$th nearest neighbor among $\mathcal{X}_{N_2}$ data points for each $\mathcal{X}_{N_1}$ data point, requires $\mathcal{O}(N_1 N_2 d)$ time complexity. Moreover, the

space complexity of the training phase is $\mathcal{O}(N_2 d)$ since $N_2$ data instances need to be saved for the testing phase.

While the training phase can be offline, the testing phase performs real-time anomaly detection. Therefore, the complexity of online testing is critical due to scalability. In the online test phase, the expensive part is to compute the $k$th nearest neighbor distance of $d$ dimensional test point to all $N_2$ points. The time and space complexity of the proposed method in the online test phase is $\mathcal{O}(N_2 d)$.

## 5. Performance Evaluation

In this section, we evaluate the performance of the proposed IDSs using a real dataset for an FDI attack and simulated data for a DDoS attack.

### *5.1. Detection Results for FDI Attack*

#### 5.1.1. Experiment Setup

We use the Warrigal dataset, which was collected by the University of Sydney in an industrial area over a period of three months with 1 Hz resolution [63]. Each message in the dataset consists of position, speed, and direction information. Position information is given in three dimensions, easting, northing, and altitude in meters. Speed and direction values are provided in meters/second and degrees, respectively. The histograms of the training data for position (easting), speed, and direction are shown in Figure 5. Due to the heterogeneity, it is not tractable to estimate the joint distribution for parametric methods. Since our IDS runs at an RSU, we consider only a portion of available data, which are collected from a few km road range, where RSU is assumed to be located at the center.

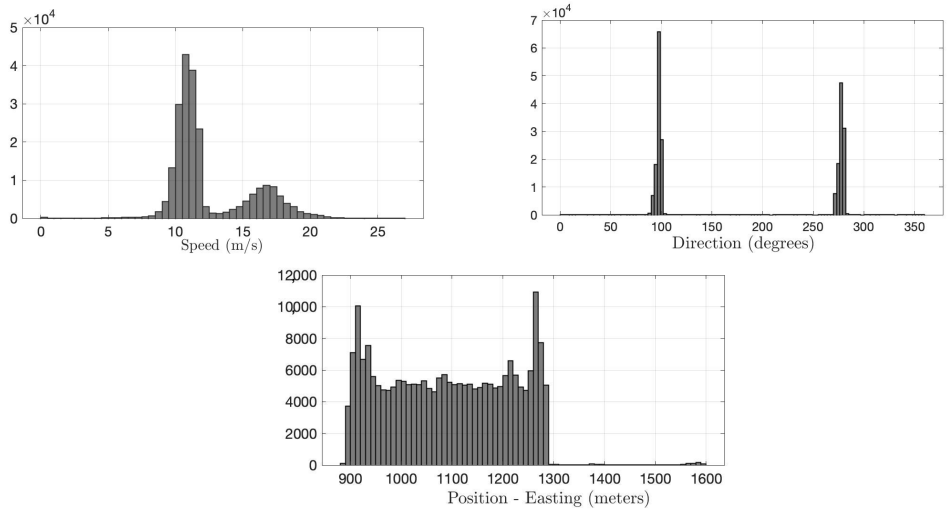


**Figure 5.** The heterogeneous probability distributions of message content in the Warrigal dataset. Histograms are obtained from the training set.

In order to generate the FDI attack scenarios, we separately injected anomalous data to each dimension generated from a uniform distribution. In each scenario, anomalous data are injected into one of the data dimensions of a randomly selected set of vehicles (i.e., attacking vehicles). For instance, an attacking vehicle only falsifies its position while broadcasting to the VANET. Falsifying multiple message dimensions is also possible, but since detecting such a case would be easier, we only considered attacks on single data contained in our experiments. Based on the nominal rates in the Warrigal dataset, anomaly rates for position and direction are selected as 30% and 40% of the nominal values, respectively. These anomaly rates reflect the attackers' objective of disrupting integrity with wrong information while remaining undetected as much as possible. Similarly to in speed, after anomaly injection, the falsified values of attacking vehicles go up to 22 m/s (50 mph), which is still in the nominal range of training data, as shown in Figure 5. Note

that even slight falsification in speed, position, and direction from multiple vehicles can cause trouble in RSU's traffic management, as well as other vehicles' decisions. To create a challenging scenario for detection and localization, in each test, the anomaly is inserted in one of the message dimensions for only 20 s.

#### 5.1.2. Results

We compare the performance of proposed IDS on FDI attacks with state-of-the-art sequential and voting-based methods in the literature.

We start with comparing the quick and accurate detection performance of the proposed IDS with an idealized version of the state-of-the sequential detector, G-CUSUM, which fits a probability distribution to nominal data and somehow exactly knows the attack magnitudes in the anomalous data. In practice, it is not tractable for G-CUSUM to know the actual attack magnitudes. Since the data distribution for each dimension in Figure 5 is close to a mixture of two Gaussian distributions, G-CUSUM assumes a Gaussian Mixture Model (GMM) type of probability distribution for both nominal and anomaly data. Three FDI attack scenarios are investigated for anomalies in the speed, position, and direction data, the results of which are given in Figure 6. The data-driven nature of the proposed IDS enables much quicker detection while satisfying the same false alarm rates compared to G-CUSUM. The proposed IDS learns the nominal baseline from data and detects the deviations from this baseline, whereas G-CUSUM suffers from the mismatches between the assumed and actual probability distributions for the nominal and anomalous data.

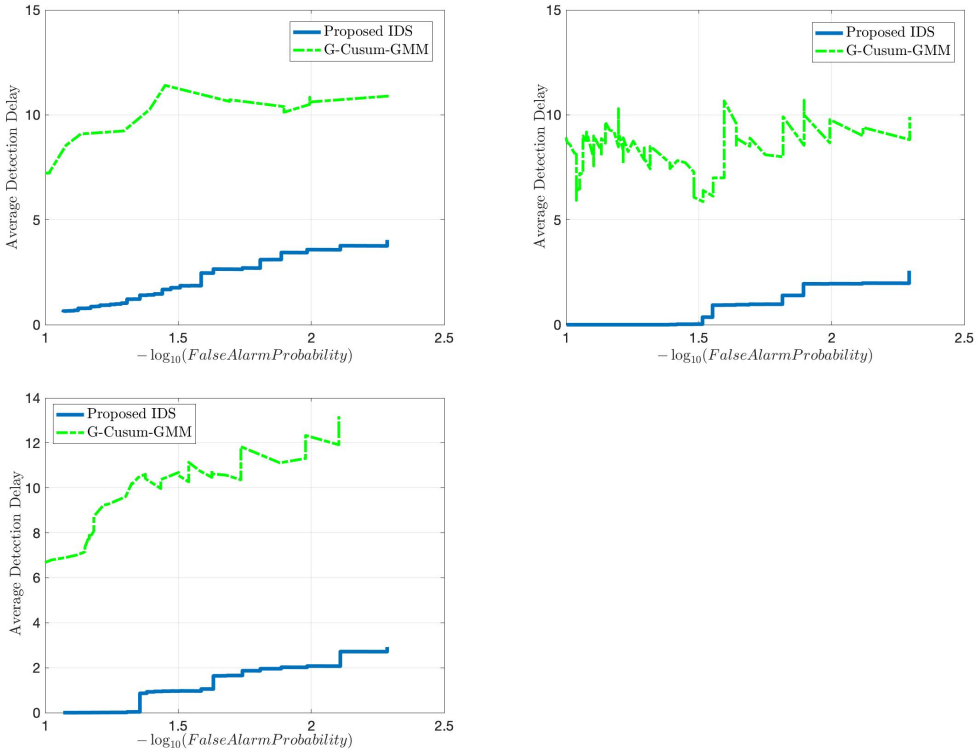


**Figure 6.** Comparison in terms of quick and accurate detection between the proposed detector and an idealized version of the state-of-the-art sequential detector (G-CUSUM), which exactly knows the attack magnitudes under different FDI attack scenarios: speed anomaly (top left), position (easting) anomaly (top right), direction anomaly (bottom).

Since voting-based IDS is a popular choice in the literature, we next compare the proposed IDS with a number of voting-based IDSs, namely HBID [26], ELIDV [24], and DCMD [20]. These systems run on each vehicle where each received message content is examined with a voting scheme. The main performance difference between such models and the proposed IDS is that while the detection accuracy for these systems decreases

with an increasing number of anomalous vehicles due to the inherent rules of voting, the proposed IDS is not affected since each vehicle is monitored at the RSU. This fact is illustrated in Figure 7 in terms of true positive rate and false positive rate considering the anomalous speed scenario. The proposed detector achieves 100% detection (true positive rate) and 0% false alarm (false positive rate) within 12 s in the considered FDI attacks, regardless of the number of attackers. Whereas the performance of voting schemes quickly degrades after the percentage of attackers in the entire vehicle population reaches a certain threshold.

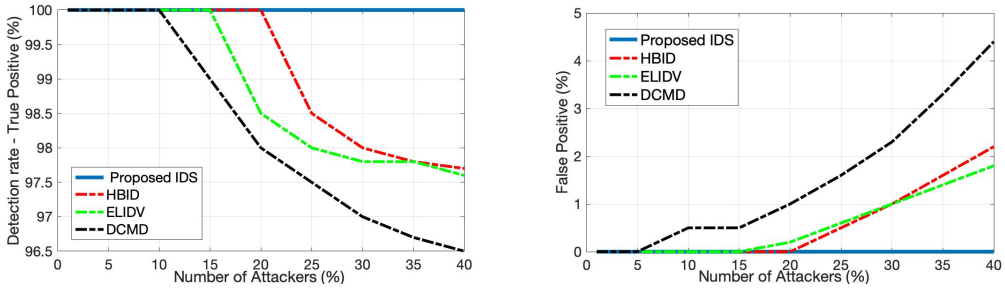


**Figure 7.** Comparison considering FDI attack in speed values between the proposed detector and several voting-based detectors from the literature.

### *5.2. Detection Results for DDoS Attack*

#### 5.2.1. Experiment Setup

In this section, we evaluate the performance of the proposed IDS for stealthy DDoS attacks targeting the availability of VANET communications. As shown in Figure 3, we split an RSU range into a number of road segments with equal lengths. The total number of received messages from a road segment in a time interval (message rate) gives the data dimension from that road segment, which mainly depends on the number of vehicles and the speed of the vehicles. For example, if traffic flow decreases, leading to a rise in the number of vehicles on the road, the message rate from the road segments increases.

For the simulation study, we use three frameworks together: OMNET++ [64], SUMO [65], and Veins [66]. OMNET++, which is a general network simulator, creates a VANET environment. Simulation of Urban Mobility (SUMO) and Veins are the two supportive frameworks, where SUMO provides a mobility model for VANET and Veins creates an interface between SUMO and OMNET++. While vehicles are moving on the roads in SUMO, they are identified as a mobile node in OMNET++ by the help of Veins. We based our simulations on the IEEE 802.11p vehicular communication protocol [67], but since our model does not specify any communication protocol, our DDoS detection algorithm can be used with other protocols as well.

We simulate a realistic scenario with SUMO by using a real road map, which is a small section of Fowler Ave. next to the University of South Florida (USF) campus in Tampa, Florida (See Figure 8). The selected road section is partitioned into 20 segments with 50 m of width for each road segment. In order to have a realistic dataset, there is no restriction on vehicular movements; all vehicles follow their randomly generated routes, i.e., they can join or leave the main road at any intersection. The average number of vehicles in the simulation area is 250.

With the given simulation parameters in Table 1, 4 h of traffic is observed for learning the training baseline, and 33.3 h of traffic is observed for test purposes. After saving all the log files, data rates for each road segment are calculated on MATLAB, and 600 test trials of 200-s duration are obtained. We generated anomaly data in MATLAB from a uniform distribution for two different DDoS attack scenarios. We consider 0.3 times mean increase for the first scenario and 1.5 times mean increase for the second scenario with respect to the corresponding nominal baseline. Anomalies are inserted on top of the nominal data in 2 of the 20 road segments from the 181st s to the 200th s.

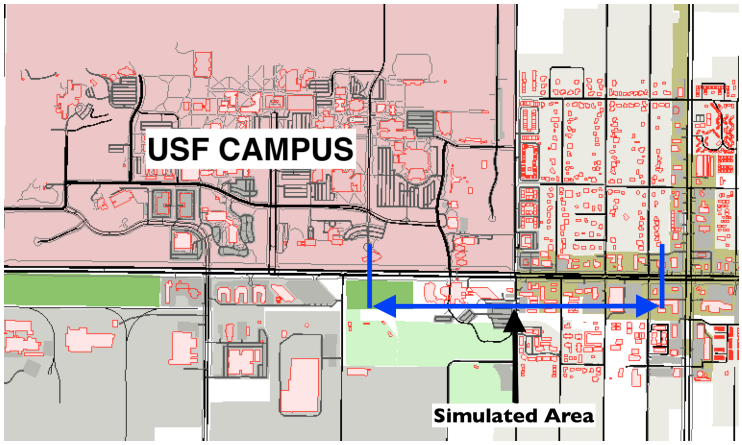


**Figure 8.** Simulation map showing Fowler Ave.

**Table 1.** Simulation Parameters.

| | |
|---|---|
| Simulation Area | 9000 × 5000 $m^2$ |
| Simulation Time (Each Trial) | 200 s |
| Number of Trials | 600 |
| Average Number of Vehicle | 250 |
| Traffic Generation | Random |
| Route Generation | Random |
| Network Protocol | IEEE 802.11p |
| Beacon Rate | 1 s |
| Network Interface | OMNET++ |
| Network Mobility Framework | Veins |
| Traffic Generator | SUMO |
| Map | Fowler Av. Tampa, FL |

#### 5.2.2. Results

We compare the proposed IDS with the state-of-the-art sequential G-CUSUM detector, e.g., [68], and the data filtering method, e.g., [41]. G-CUSUM assumes a probability distribution for nominal and anomalous data, whereas the data filtering approach looks for an increase in the total data rate received by RSU without performing any statistical analysis. In Figures 9 and 10, it is seen that the observations from the two road segments to which the anomaly is added follow different distributions. While the distribution of one road segment is similar to a negative binomial (Figure 9), which is indeed a Poisson distribution with conjugate prior (i.e., Gamma distribution) on the rate parameter, the distribution of other road segments is similar to Gaussian (Figure 10). Hence, we examine two idealized versions of G-CUSUM, which fit negative binomial and Gaussian distributions for each road segment and somehow exactly know the attack magnitudes of 30% and 150%.

For both attack scenarios with 30% and 150% average mean increase from the nominal mean rate, Figures 11 and 12 show that the proposed IDS outperforms the G-CUSUM approach and the data filtering approach in terms of quick, accurate detection. In particular, the proposed IDS achieves a much smaller average detection delay while satisfying the same false alarm rates (e.g., for 0.01 false alarm rate, approximately 1/2 times and 1/5 times in Figures 11 and 12). Moreover, the G-CUSUM and data filtering approaches have certain practical disadvantages compared to the proposed IDS. The data filtering method can only detect such low-rate stealthy attacks by monitoring the total number of packets received

by the RSU since the individual data rates from road segments still appear to be harmless to the network. As a result, it is not tractable for the data filtering method to localize and mitigate the attack. For G-CUSUM, indeed, there is no way to exactly know the actual attack magnitudes. In practice, a number of parallel tests with different assumptions for the attack magnitude can be applied; however, even for the best test that alarms first, the mismatch between the assumed anomaly distribution and the actual distribution would cause significant performance degradation. As shown in Figures 11 and 12, even the ideal G-CUSUM, which exactly knows the attack magnitude, suffers from deviations in the observed data from the assumed probability distributions. Furthermore, G-CUSUM inevitably follows a univariate approach by assuming independence between road segments [69] since it does not know which road segments will include anomalies. The multivariate nature of the proposed detector also facilitates its superior performance.

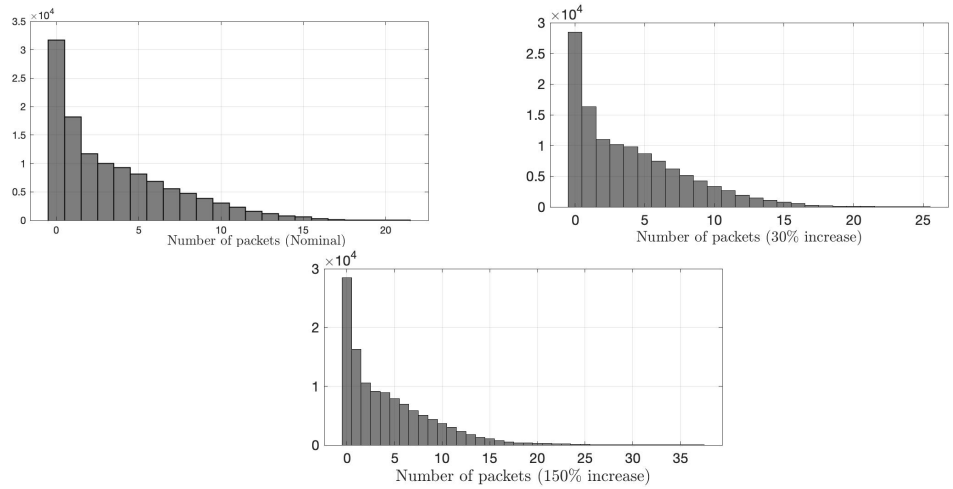


**Figure 9.** Histogram of number of packets for a road segment. The first histogram represents the distribution of nominal data, whereas the second and third represent attack cases with an average increase that is 0.3 and 1.5 times the baseline, respectively. Nominal and attack distributions are close to a negative binomial distribution with extended tails under attacks.

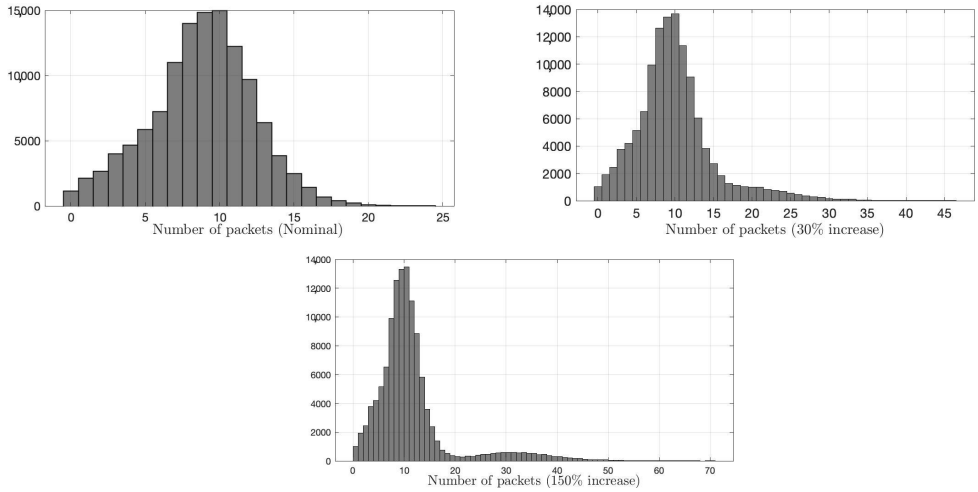


**Figure 10.** Histogram of number of packets for a road segment. The first histogram represents the distribution of nominal data, whereas the second and third represent attack cases an average increase that is 0.3 and 1.5 times the baseline, respectively. Nominal and attack distributions are close to a normal distribution with extended tails under attacks.

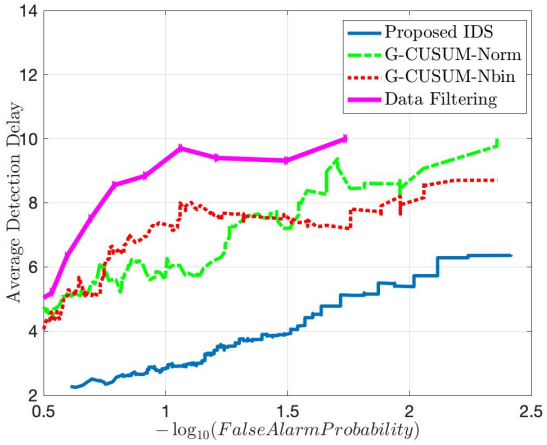


**Figure 11.** Comparison in terms of quick and accurate detection for an average DDoS attack magnitude of 0.3 times the nominal mean data rate between the proposed method, two idealized G-CUSUM variants that know the exact attack magnitude, and the data filtering method.

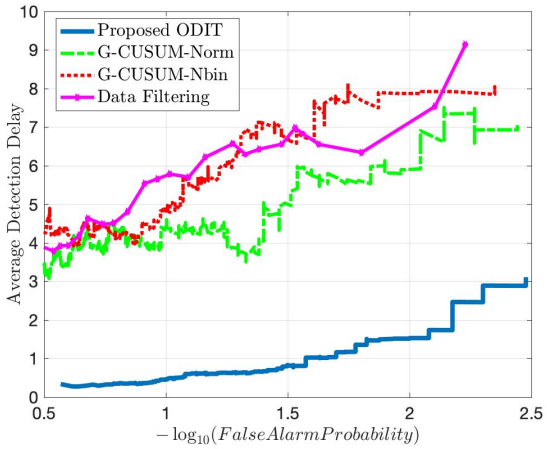


**Figure 12.** Comparison in terms of quick and accurate detection for an average DDoS attack magnitude of 1.5 times the nominal mean data rate between the proposed method, two idealized G-CUSUM variants which know the exact attack magnitude, and the data filtering method.

### *5.3. Localization Results*

We next evaluate the attack localization performance of the proposed IDS using the receiver operating characteristic (ROC) curves, which present the achieved true positive rates while the algorithm satisfies different levels of false positive constraints. First, we consider the identification of attacking vehicles in the FDI attack scenario (anomalous speed case). Since, in this case, the proposed detector is applied to each vehicle, and the messages include the vehicle ID, there is no need for a separate vehicle identification mechanism after detection. Specifically, once the proposed IDS alarms a vehicle, this vehicle is automatically identified as attacking. In the anomalous speed scenario, by selecting the detection threshold as $h = 2$ in all test trials, the proposed IDS achieves zero false alarms for non-attacking vehicles and 100% correct detection of attacking vehicles with a maximum delay of 12 s (Figure 13). We next consider the identification of anomalous data dimension using the localization strategy given in (6) and summarized by Algorithm 1. Figure 13 displays the perfect detection of the anomalous speed data while satisfying zero false alarms in all test trials.

Finally, the identification of road segments in the DDoS attack scenario using Algorithm 1 is considered. As demonstrated by Figure 13, the proposed IDS successfully identifies the anomalous road segments with a high correct detection rate (e.g., 94%) while satisfying a small false alarm rate (e.g., 5%).

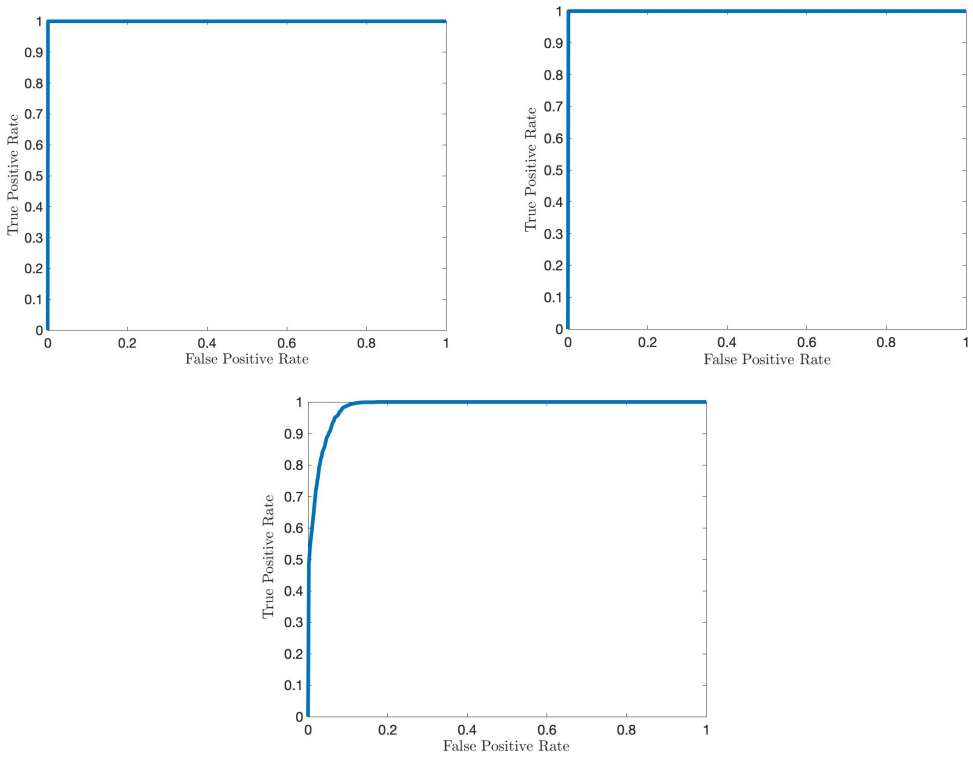


**Figure 13.** ROC curves for the proposed IDS's anomaly localization performance: identification of anomalous vehicles in FDI attack to speed data (**top left**), identification of anomalous data in FDI attack to speed data (**top right**), and identification of anomalous road segments in DDoS attack (**bottom**).

## 6. Conclusions

We proposed a statistical non-parametric intrusion detection system (IDS) for the online detection of false data injection (FDI) attacks and distributed denial-of-service (DDoS) attacks. The proposed system runs roadside unit (RSU) monitoring to broadcasted messages from the vehicles in its range. To be specific, in the FDI attack case, we considered the (ID, speed, position, direction) message format; however, the proposed IDS is based on a generic anomaly detection algorithm, and thus easily extends to other data types. Similarly, the IDS proposed for DDoS attacks is applicable to any data type and communication protocol as it monitors the data rates (i.e., number of packets in unit time) from a number of road segments. An attack localization procedure was also proposed to follow up on an alarm raised by the detection procedure. As the final stage in attack mitigation, RSU drops the identified messages from identified vehicles for FDI attacks and from identified road segments for DDoS attacks. The detection and localization performances of the proposed IDS are evaluated in the FDI and stealthy DDoS cases using a real traffic dataset called the Warrigal dataset, and state-of-the-art traffic simulators, respectively. To the best of our knowledge, this work is the first to use a real dataset in VANET cybersecurity. The experimental results demonstrated the superior performance of the proposed IDS in terms of quick and accurate detection and localization compared to state-of-the-art voting schemes, parametric sequential change detection algorithm, and the data filtering method. In future work, we plan to extend the proposed IDS to other attack types and specifically designed sporadic attacks, which aim to avoid detection by sequential detectors such as our proposed detector. Since our sequential detector looks for continuous anomalies that would cause decision statistics to rise and trigger an alarm, carefully staged short-duration frequent attacks may bypass our detector by preventing the decision statistic from reaching the detection threshold. While such sporadic attacks cannot be as impactful as continuous

attacks within the same duration, they may eventually damage the targeted system if they remain undetected.

**Author Contributions:** Conceptualization, A.H. and Y.Y.; methodology, Y.Y.; software, A.H.; validation, A.H. and Y.Y.; formal analysis, Y.Y.; investigation, A.H. and Y.Y.; resources, A.H. and Y.Y.; data curation, A.H.; writing—original draft preparation, A.H.; writing—review and editing, Y.Y.; visualization, A.H.; supervision, Y.Y.; project administration, Y.Y.; funding acquisition, Y.Y. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by National Science Foundation (NSF) grant number 2040572.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** The Warrigal dataset [63] can be found at http://its.acfr.usyd.edu.au/datasets-2/warrigal/, accessed on 29 August 2022.

**Conflicts of Interest:** The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

## Appendix A

The proof of Theorem 1 is based on an upper bound, $FAR \leq e^{-\omega_0 h}$, for the false alarm rate of CUSUM-like algorithms with independent increments [58], such as the proposed IDS. Here, $\omega_0 \geq 0$ is the solution to $E[e^{\omega_0 D_t}] = 1$. Given a false alarm constraint $\beta$, the threshold $h$ can be set using $\beta = e^{-\omega_0 h}$ to ensure that $FAR \leq \beta$. Hence, we get the equation $h = \frac{-\log \beta}{\omega_0}$, where we need to find $\omega_0$ from $E[e^{\omega_0 D_t}] = 1$.

We first derive the asymptotic distribution of the anomaly evidence $D_t$ in the absence of anomalies. Its cumulative distribution function is given by

$$P(D_t \leq y) = P((L_t)^d \leq (L_{(M)})^d + y).$$

It is sufficient to find the probability distribution of $(L_t)^d$, the $d$th power of the $k$NN distance at time $t$. Independent $d$-dimensional instances $\{\boldsymbol{x}_t\}$ form a Poisson point process over time. The nearest neighbor ($k = 1$) distribution for a Poisson point process is given by

$$P(L_t \leq r) = 1 - \exp(-\Lambda(b(\boldsymbol{x}_t, r)))$$

where $\Lambda(b(\boldsymbol{x}_t, r))$ is the arrival intensity (i.e., Poisson rate measure) in the $d$-dimensional hypersphere $b(\boldsymbol{x}_t, r)$ centered at $\boldsymbol{x}_t$ with radius $r$ [70]. Asymptotically, for a large number of training instances as $N_2 \to \infty$, under the null (nominal) hypothesis, the nearest neighbor distance $L_t$ of $\boldsymbol{x}_t$ takes small values, defining an infinitesimal hyperball with homogeneous intensity $\lambda = 1$ around $\boldsymbol{x}_t$. Since for a homogeneous Poisson process the intensity is written as $\Lambda(b(\boldsymbol{x}_t, r)) = \lambda |b(\boldsymbol{x}_t, r)|$ [70], where $|b(\boldsymbol{x}_t, r)| = \frac{\pi^{d/2}}{\Gamma(d/2+1)} r^d = v_d r^d$ is the Lebesgue measure (i.e., $d$-dimensional volume) of the hyperball $b(\boldsymbol{x}_t, r)$, we rewrite the nearest neighbor distribution as

$$P(L_t \leq r) = 1 - \exp\left(-v_d r^d\right),$$

where $v_d = \frac{\pi^{d/2}}{\Gamma(d/2+1)}$ is the constant for the $d$-dimensional Lebesgue measure.

Now, applying a change in variables we can write the probability density of $(L_t)^d$ and $D_t$ as

$$\begin{aligned} f_{(L_t)^d}(y) &= \frac{\partial}{\partial y}[1-\exp(-v_d y)], \\ &= v_d \exp(-v_d y), \\ f_{D_t}(y) &= v_d \exp(-v_d (L_t)^d) \exp(-v_d y) \end{aligned} \tag{A1}$$

Using the probability density derived in (A1), $E[e^{\omega_0 D_t}] = 1$ can be written as

$$\begin{aligned} 1 &= \int_{-(L_{(M)})^d}^{\phi} e^{\omega_0 y} v_d e^{-v_d (L_t)^d} e^{-v_d y} dy, \\ \frac{e^{v_d (L_{(M)})^d}}{v_d} &= \int_{-(L_{(M)})^d}^{\phi} e^{(\omega_0 - v_d) y} dy, \\ &= \frac{e^{(\omega_0 - v_d) y}}{\omega_0 - v_d}\Bigg|_{-(L_{(M)})^d}^{\phi}, \\ &= \frac{e^{(\omega_0 - v_d)\phi} - e^{(\omega_0 - v_d)(-(L_{(M)})^d)}}{\omega_0 - v_d}, \end{aligned} \tag{A2}$$

where $-(L_{(M)})^d$ and $\phi$ are the lower and upper bounds for $D_t = (L_t)^d - (L_{(M)})^d$. The upper bound $\phi$ is obtained from the training set.

As $N_2 \to \infty$, since the $d$th power of $(1-\alpha)$th percentile of nearest neighbor distances in the training set goes to zero, i.e., $(L_{(M)})^d \to 0$, we have

$$e^{(\omega_0 - v_d)\phi} = \frac{e^{v_d (L_{(M)})^d}}{v_d}(\omega_0 - v_d) + 1.$$

We next rearrange the terms to obtain the form of $e^{\phi x} = a_0(x + \theta)$ where $x = \omega_0 - v_d$, $a_0 = \frac{e^{v_d (L_{(M)})^d}}{v_d}$, and $\theta = \frac{v_d}{e^{v_d (L_{(M)})^d}}$. The solution for $x$ is given by the Lambert-W function [71] as $x = -\theta - \frac{1}{\phi}\mathcal{W}(-\phi e^{-\phi\theta}/a_0)$, hence

$$\omega_0 = v_d - \theta - \frac{1}{\phi}\mathcal{W}\left(-\phi\theta e^{-\phi\theta}\right).$$

## References


1. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANet security challenges and solutions: A survey. *Veh. Commun.* **2017**, *7*, 7–20. [CrossRef]
2. Amoozadeh, M.; Raghuramu, A.; Chuah, C.N.; Ghosal, D.; Zhang, H.M.; Rowe, J.; Levitt, K. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Commun. Mag.* **2015**, *53*, 126–132. [CrossRef]
3. Hakak, S.; Gadekallu, T.R.; Ramu, S.P.; Maddikunta, P.K.R.; de Alwis, C.; Liyanage, M. Autonomous Vehicles in 5G and beyond: A Survey. *arXiv* **2022**, arXiv:2207.10510.
4. Uhlemann, E. The battle of technologies or the battle of business models?[Connected vehicles]. *IEEE Veh. Technol. Mag.* **2018**, *13*, 14–18. [CrossRef]
5. Mannoni, V.; Berg, V.; Sesia, S.; Perraud, E. A comparison of the V2X communication systems: ITS-G5 and C-V2X. In Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019; pp. 1–5.
6. Lee, J.; Ahn, S. Adaptive Configuration of Mobile Roadside Units for the Cost-Effective Vehicular Communication Infrastructure. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 6594084. [CrossRef]
7. Alrehan, A.M.; Alhaidari, F.A. Machine Learning Techniques to Detect DDoS Attacks on VANET System: A Survey. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 19–21 March 2019; pp. 1–6. [CrossRef]

8. Xu, X.; Wang, Y.; Wang, P. Comprehensive Review on Misbehavior Detection for Vehicular Ad Hoc Networks. *J. Adv. Transp.* **2022**, *2022*, 4725805. [CrossRef]
9. Soleymani, S.A.; Abdullah, A.H.; Hassan, W.H.; Anisi, M.H.; Goudarzi, S.; Baee, M.A.R.; Mandala, S. Trust management in vehicular ad hoc network: A systematic review. *EURASIP J. Wirel. Commun. Netw.* **2015**, *2015*, 146. [CrossRef]
10. Khan, U.; Agrawal, S.; Silakari, S. A detailed survey on misbehavior node detection techniques in vehicular ad hoc networks. In *Information Systems Design and Intelligent Applications*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 11–19.
11. Zhang, C.; Cai, Z.; Chen, W.; Luo, X.; Yin, J. Flow level detection and filtering of low-rate DDoS. *Comput. Netw.* **2012**, *56*, 3417–3431. doi: 10.1016/j.comnet.2012.07.003. [CrossRef]
12. Chen, Z.; Yeo, C.K.; Lee, B.S.; Lau, C.T. Power spectrum entropy based detection and mitigation of low-rate DoS attacks. *Comput. Netw.* **2018**, *136*, 80–94. [CrossRef]
13. Boualouache, A.; Engel, T. A Survey on Machine Learning-based Misbehavior Detection Systems for 5G and Beyond Vehicular Networks. *arXiv* **2022**, arXiv:2201.10500.
14. Wahab, O.A.; Otrok, H.; Mourad, A. A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles. *Comput. Commun.* **2014**, *41*, 43–54. [CrossRef]
15. Li, X.; Liu, J.; Li, X.; Li, H. A reputation-based secure scheme in vehicular ad hoc networks. *Int. J. Grid Util. Comput.* **2015**, *6*, 83–90. [CrossRef]
16. van der Heijden, R.W.; Dietzel, S.; Leinmüller, T.; Kargl, F. Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 779–811. [CrossRef]
17. Wex, P.; Breuer, J.; Held, A.; Leinmuller, T.; Delgrossi, L. Trust issues for vehicular ad hoc networks. In Proceedings of the Vehicular Technology Conference, Singapore, 11–14 May 2008; pp. 2800–2804.
18. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. Misbehavior detection and efficient revocation within VANET. *J. Inf. Secur. Appl.* **2019**, *46*, 193–209. [CrossRef]
19. Abhishek, N.V.; Lim, T.J. Trust-based adversary detection in edge computing assisted vehicular networks. *J. Commun. Netw.* **2022**, *24*, 451–462. [CrossRef]
20. Ruj, S.; Cavenaghi, M.A.; Huang, Z.; Nayak, A.; Stojmenovic, I. On data-centric misbehavior detection in VANETs. In Proceedings of the Vehicular Technology Conference (VTC Fall), San Francisco, CA, USA, 5–8 September 2011; pp. 1–5.
21. Ghaleb, F.A.; Maarof, M.A.; Zainal, A.; Al-Rimy, B.A.S.; Saeed, F.; Al-Hadhrami, T. Hybrid and Multifaceted Context-Aware Misbehavior Detection Model for Vehicular Ad Hoc Network. *IEEE Access* **2019**, *7*, 159119–159140. [CrossRef]
22. Sharshembiev, K.; Yoo, S.M.; Elmahdi, E.; Kim, Y.K.; Jeong, G.H. Fail-Safe Mechanism Using Entropy Based Misbehavior Classification and Detection in Vehicular Ad Hoc Networks. In Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 14–17 July 2019, pp. 123–128.
23. Guo, J.; Li, X.; Liu, Z.; Ma, J.; Yang, C.; Zhang, J.; Wu, D. TROVE: A context-awareness trust model for VANETs using reinforcement learning. *IEEE Internet Things J.* **2020**, *7*, 6647–6662. [CrossRef]
24. Sedjelmaci, H.; Senouci, S.M.; Abu-Rgheff, M.A. An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks. *IEEE Internet Things J.* **2014**, *1*, 570–577. [CrossRef]
25. Sedjelmaci, H.; Senouci, S.M.; Bouali, T. Predict and prevent from misbehaving intruders in heterogeneous vehicular networks. *Veh. Commun.* **2017**, *10*, 74–83. [CrossRef]
26. Zaidi, K.; Milojevic, M.B.; Rakocevic, V.; Nallanathan, A.; Rajarajan, M. Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection. *IEEE Trans. Veh. Technol.* **2016**, *65*, 6703–6714. [CrossRef]
27. Liang, J.; Lin, Q.; Chen, J.; Zhu, Y. A Filter Model Based on Hidden Generalized Mixture Transition Distribution Model for Intrusion Detection System in Vehicle Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2019**, *10*, 2707–2722. [CrossRef]
28. Eziama, E.; Tepe, K.; Balador, A.; Nwizege, K.S.; Jaimes, L.M. Malicious Node Detection in Vehicular Ad-Hoc Network Using Machine Learning and Deep Learning. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.
29. So, S.; Sharma, P.; Petit, J. Integrating Plausibility Checks and Machine Learning for Misbehavior Detection in VANET. In Proceedings of the 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA, 17–20 December 2018; pp. 564–571. [CrossRef]
30. Gyawali, S.; Qian, Y. Misbehavior Detection using Machine Learning in Vehicular Communication Networks. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
31. Nguyen, V.L.; Lin, P.C.; Hwang, R.H. Enhancing misbehavior detection in 5G vehicle-to-vehicle communications. *IEEE Trans. Veh. Technol.* **2020**, *69*, 9417–9430. [CrossRef]
32. van der Heijden, R.W.; Lukaseder, T.; Kargl, F. Veremi: A dataset for comparable evaluation of misbehavior detection in vanets. In Proceedings of the International Conference on Security and Privacy in Communication Systems, Singapore, 8–10 August 2018; pp. 318–337.
33. So, S.; Petit, J.; Starobinski, D. Physical Layer Plausibility Checks for Misbehavior Detection in V2X Networks. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, Miami, FL, USA, 15–17 May 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 84–93. [CrossRef]

34. Singh, P.K.; Gupta, S.; Vashistha, R.; Nandi, S.K.; Nandi, S. Machine Learning Based Approach to Detect Position Falsification Attack in VANETs. In Proceedings of the International Conference on Security & Privacy, Jaipur, India, 9–11 January 2019; pp. 166–178.
35. Sharma, P.; Liu, H. A machine-learning-based data-centric misbehavior detection model for internet of vehicles. *IEEE Internet Things J.* **2020**, *8*, 4991–4999. [CrossRef]
36. Ercan, S.; Ayaida, M.; Messai, N. Misbehavior detection for position falsification attacks in VANETs using machine learning. *IEEE Access* **2021**, *10*, 1893–1904. [CrossRef]
37. Ullah, S.; Khan, M.A.; Ahmad, J.; Jamal, S.S.; e Huma, Z.; Hassan, M.T.; Pitropakis, N.; Buchanan, W.J. HDL-IDS: A hybrid deep learning architecture for intrusion detection in the Internet of Vehicles. *Sensors* **2022**, *22*, 1340. [CrossRef] [PubMed]
38. Yu, Y.; Zeng, X.; Xue, X.; Ma, J. LSTM-Based Intrusion Detection System for VANETs: A Time Series Classification Approach to False Message Detection. *IEEE Trans. Intell. Transp. Syst.* **2022**, 1–13 . [CrossRef]
39. Parkinson, S.; Ward, P.; Wilson, K.; Miller, J. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2898–2915. [CrossRef]
40. Soryal, J.; Saadawi, T. DoS attack detection in Internet-connected vehicles. In Proceedings of the 2013 International Conference on Connected Vehicles and Expo (ICCVE), Las Vegas, NV, USA, 2–6 December 2013; pp. 7–13. [CrossRef]
41. Verma, K.; Hasbullah, H.; Kumar, A. Prevention of DoS attacks in VANET. *Wirel. Pers. Commun.* **2013**, *73*, 95–126. [CrossRef]
42. Mokdad, L.; Ben-Othman, J.; Nguyen, A.T. DJAVAN: Detecting jamming attacks in Vehicle Ad hoc Networks. *Perform. Eval.* **2015**, *87*, 47–59. [CrossRef]
43. Kerrache, C.A.; Lagraa, N.; Calafate, C.T.; Lakas, A. TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs. *Veh. Commun.* **2017**, *9*, 254–267. [CrossRef]
44. Zhang, T.; Xu, C.; Zou, P.; Tian, H.; Kuang, X.; Yang, S.; Zhong, L.; Niyato, D. How to Mitigate DDoS Intelligently in SD-IoV: A Moving Target Defense Approach. *IEEE Trans. Ind. Inform.* **2022**, 1–10 . [CrossRef]
45. Gaurav, A.; Gupta, B.; Peñalvo, F.J.G.; Nedjah, N.; Psannis, K. Ddos attack detection in vehicular ad-hoc network (vanet) for 5g networks. In *Security and Privacy Preserving for IoT and 5G Networks*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 263–278.
46. Karagiannis, D.; Argyriou, A. Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning. *Veh. Commun.* **2018**, *13*, 56–63. [CrossRef]
47. Lyamin, N.; Kleyko, D.; Delooz, Q.; Vinel, A. AI-Based Malicious Network Traffic Detection in VANETs. *IEEE Netw.* **2018**, *32*, 15–21. [CrossRef]
48. Kolandaisamy, R.; Md Noor, R.; Ahmedy, I.; Ahmad, I.; Reza Z'aba, M.; Imran, M.; Alnuem, M. A multivariant stream analysis approach to detect and mitigate DDoS attacks in vehicular ad hoc networks. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 2874509. [CrossRef]
49. Türkoğlu, M.; Polat, H.; Koçak, C.; Polat, O. Recognition of DDoS Attacks on SD-VANET Based on Combination of Hyperparameter Optimization and Feature Selection. *Expert Syst. Appl.* **2022**, *203*, 117500. [CrossRef]
50. Adhikary, K.; Bhushan, S.; Kumar, S.; Dutta, K. Hybrid algorithm to detect DDoS attacks in VANETs. *Wirel. Pers. Commun.* **2020**, *114*, 3613–3634. [CrossRef]
51. Kadam, N.; Krovi, R.S. Machine Learning Approach of Hybrid KSVN Algorithm to Detect DDoS Attack in VANET. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*. [CrossRef]
52. Anyanwu, G.O.; Nwakanma, C.I.; Lee, J.M.; Kim, D.S. Optimization of RBF-SVM Kernel using Grid Search Algorithm for DDoS Attack Detection in SDN-based VANET. *IEEE Internet Things J.* **2022**. [CrossRef]
53. Haydari, A.; Yilmaz, Y. Real-Time Detection and Mitigation of DDoS Attacks in Intelligent Transportation Systems. In Proceedings of the 2018 21st International Conference on Intelligent Transportation Systems (ITSC), Maui, HI, USA, 4–7 November 2018; pp. 157–163.
54. Wahab, O.A.; Mourad, A.; Otrok, H.; Bentahar, J. CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks. *Expert Syst. Appl.* **2016**, *50*, 40–54. [CrossRef]
55. Yu, B.; Xu, C.Z.; Xiao, B. Detecting sybil attacks in VANETs. *J. Parallel Distrib. Comput.* **2013**, *73*, 746–756. [CrossRef]
56. Nexusguard. DDoS Threat Report 2019 Q3 [Online]. Available online: https://tinyurl.com/25juf7ma (accessed on 29 August 2022).
57. Baker, M. Statisticians issue warning over misuse of P values. *Nature* **2016**, *531*, 151. [CrossRef] [PubMed]
58. Basseville, M.; Nikiforov, I.V. *Detection of Abrupt Changes: Theory and Application*; Prentice Hall: Englewood Cliffs, NJ, USA, 1993; Volume 104.
59. Poor, H.V.; Hadjiliadis, O. *Quickest Detection*; Cambridge University Press: Cambridge, UK, 2009; Volume 40.
60. Yilmaz, Y. Online nonparametric anomaly detection based on geometric entropy minimization. In Proceedings of the 2017 IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, 25–30 June 2017; pp. 3010–3014.
61. Hero, A.O. Geometric entropy minimization (GEM) for anomaly detection and localization. In Proceedings of the Advances in Neural Information Processing Systems, Vancouver, BC, Canada, 3–6 December 2007; pp. 585–592.
62. Poor, H.V. *An Introduction to Signal Detection and Estimation*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2013.
63. Ward, J.; Worrall, S.; Agamennoni, G.; Nebot, E. The warrigal dataset: Multi-vehicle trajectories and v2v communications. *IEEE Intell. Transp. Syst. Mag.* **2014**, *6*, 109–117. [CrossRef]

64. Varga, A.; Hornig, R. An overview of the OMNeT++ simulation environment. In Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops, Marseille, France, 3–7 March 2008; p. 60.
65. Behrisch, M.; Bieker, L.; Erdmann, J.; Krajzewicz, D. SUMO–simulation of urban mobility: An overview. In Proceedings of the SIMUL 2011, The Third International Conference on Advances in System Simulation, ThinkMind, Barcelona, Spain, 23–29 October 2011.
66. Sommer, C.; German, R.; Dressler, F. Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis. *IEEE Trans. Mob. Comput.* **2011**, *10*, 3–15. [CrossRef]
67. Jiang, D.; Delgrossi, L. IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments. In Proceedings of the Vehicular Technology Conference, Singapore, 11–14 May 2008; pp. 2036–2040.
68. Guo, Y.; Lee, I. Forensic analysis of DoS attack traffic in MANET. In Proceedings of the 2010 4th International Conference on IEEE Network and System Security (NSS), Melbourne, Australia, 1–3 September 2010; pp. 293–298.
69. Mei, Y. Efficient scalable schemes for monitoring a large number of data streams. *Biometrika* **2010**, *97*, 419–433. [CrossRef]
70. Chiu, S.N.; Stoyan, D.; Kendall, W.S.; Mecke, J. *Stochastic Geometry and Its Applications*; John Wiley & Sons: Hoboken, NJ, USA, 2013.
71. Scott, T.C.; Fee, G.; Grotendorst, J. Asymptotic series of generalized Lambert W function. *ACM Commun. Comput. Algebra* **2014**, *47*, 75–83. [CrossRef]