June 2019

Statistical Anomaly Detection and Mitigation of Cyber Attacks for Intelligent Transportation Systems

Ammar Haydari
University of South Florida, ammarhaydari@mail.usf.edu

Statistical Anomaly Detection and Mitigation of Cyber Attacks for Intelligent Transportation Systems

by

Ammar Haydari

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Electrical Engineering
Department of Electrical Engineering
College of Engineering
University of South Florida

Major Professor: Yasin Yilmaz, Ph.D.
Ismail Uysal, Ph.D.
Kwang-Cheng Chen, Ph.D.

Date of Approval:
June 7, 2019

Keywords: VANET security, intrusion detection, DDoS attack, false data injection, security objectives

DEDICATION

Dedicated to the two most important persons in my life: The woman I want to build my life with - Canim Esim and the woman built my life - Canim Annem

ACKNOWLEDGMENTS

First and foremost, I would like to express my gratitude to my advisor Dr. Yasin Yilmaz who not only guided me in this very first step of academic journey but also paved my way towards to have a strong future goals.

Second, special thank goes out to Kwang-Cheng Chen and Ismail Uysal for agreeing to be in my defense committee.

I would like to express my sincere appreciation to my Turkish Ministry of National Education where I received my funding during my master education. This thesis would not be written without this great opportunity.

I am extremely grateful to my group members at University of South Florida, Keval Doshi, Mahsa Mozaffari, Salman Shuvo and Almuthanna Nassar with whom I had a great discussions.

A very special thank you goes out to my parents Ahmet and Fatma Haydari, my brothers and best friends Huseyin and Servet Haydari who never stopped believing me.

My acknowledgements would not be complete without thanking to my fiancé Sayre Nur Terzi, whose support always encouraged me.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Secure vehicular communication is a critical factor for secure traffic management. Perfect security in intelligent transportation systems (ITS) has solid and efficient intrusion detection systems (IDS). In this paper, we consider false data injection attacks and distributed denial-of-service attacks (DDoS), especially the stealth low-rate DDoS attacks, targeting the integrity and availability, respectively, in vehicular ad-hoc networks (VANET). Novel statistical intrusion detection and mitigation techniques are proposed for the considered attacks. The performance of the proposed methods are evaluated using a traffic simulator and a real traffic dataset. Comparisons with the state-of-the-art solutions clearly demonstrate the superior performance of the proposed methods in terms of quick and accurate detection and localization of cyber-attacks.

CHAPTER 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 the 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 the future traffic, as well as traditional vehicles controlled by a driver [2]. VANET applications can be classified into two types as traffic safety applications and traffic management applications. Route planning applications for drivers is an example for the traffic management applications. The safety-related applications are exemplified by road condition applications and accident information systems.

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 two essential aspects of VANET security. Static infrastructure elements placed near the road, called Roadside Units (RSUs), have a critical role in VANET. RSUs provide high connectivity and security in traffic. VANET components such as vehicles and RSUs typically use short-range and short-lived communications due to the high speed of vehicles. Considering also the potential life-threatening outcomes in traffic, cyber-attacks to VANET need to be quickly and accurately detected and mitigated. To this end, in this paper, we propose a statistical detection and mitigation method at RSU for cyber-attacks targeting both data availability and integrity.

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 to the vehicular traffic. Autonomous vehicles are exposed to an even greater risk due to false data injection (FDI) attacks as their automatic decisions may rely more on the received VANET messages. For example, position is one of the most important information in VANET; when a vehicle sends wrong position information, then a nearby autonomous vehicle may accelerate according to the received falsified message. An effective intrusion detection systems (IDS) should effectively deal with FDI attacks, in which attacker sends bogus information to the network in order to change the vehicle behaviors in traffic. Once an intruder injects bogus data to 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 [3],[4]. In this work, we propose a statistical anomaly detection method that can quickly detects FDI attacks, including the previously unseen ones, as opposed to the signature-based methods in VANET. 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 that stores the previous message contents. Once our method detects an anomalous vehicle, it blocks the data transfer from that vehicle and informs the other vehicles. This cybersecurity mechanism prevents malicious vehicles to affect the whole traffic system including public transportations and private vehicles.

1.2 DDoS Attacks Targeting Availability

Availability of the communications is one of the main objectives in ITS. Denial-of-Service (DoS) attacks target the availability of network service, e.g., by sending high volume (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. Unavailability of the VANET service due to a DoS attack may cause a significant damage to the 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 is 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 stealth DDoS attack, called low-rate DDoS attack [5], [6], that can easily bypass traditional IDSs such as data traffic filters and firewalls while still causing a significant disruption in the targeted service due to its synchronous nature.

It is quite challenging to timely detect and mitigate low-rate DDoS attacks compared to the standard DoS 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 server can be tremendous, thus, the server gets overwhelmed and stops serving legitimate users. We propose a powerful multivariate-statistical method for the timely detection and mitigation of low-rate DDoS attacks to RSU.

We summarized our contributions in this thesis in the next subsection.

1.3 Contributions

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

- A novel statistical detector is investigated for FDI and DDoS attacks against RSU.
- Based on the detection method a statistical anomaly localization, and accordingly attack mitigation method is proposed for FDI and DDoS attacks targeting RSU.
- 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 considered attack types are given in Section 3. The proposed statistical detection and mitigation methods are presented in Section 4. Numerical results are discussed in Section 5. Finally, the paper is concluded with future work in Section 6. Throughout the paper, lowercase and uppercase bold letters are used to denote vectors and matrices, respectively.

CHAPTER 2: RELATED WORKS

2.1 False Data Injection Attacks

Injection of fake messages is a high threat to ITS/VANET security [7]. There are several key features that differentiate VANET and ITS security from other network security topics, such as high mobility, dynamic characteristics, and life-threatening conditions. Trust-based and data-based methods are the most common intrusion detection approaches in VANET. Trust models are based on voting or scoring schemes in which the reliability of a node broadcasting a message is voted by the other nodes receiving the message. Once the cumulative voting score exceeds a level against the node, it is declared as intruder, and its message dissemination is blocked [8]. Data-centric detection models are used with emergency messages where behavior of the node and the received message are compared. One of the early works was presented in [9]. The authors proposed a data-centric malicious vehicle detection mechanism using specific alert messages that convey information about the emergency of traffic or emergency of the vehicle. If there is a mismatch between the received packets and the behavior of the node transmitting the packets, system raises a false data alarm, and informs other nodes about the false data and misbehaving node. In [10], a defense mechanism was proposed against several attack types including FDI attacks using vehicle reputation scores collected by RSUs. Same authors proposed a new prediction and prevention technique for VANET security in [11]. Both FDI and packet drop attacks are successfully detected and prevented using a game theory approach for predicting the future malicious vehicles, and a rule-based technique for detecting malicious vehicles from their behaviors.

In [12], authors proposed a detection mechanism doing two-level position verification by combining them with subjective logic. They improved previously proposed two position verification algorithms and defined a cumulative fusion operator in order to implement them for VANET. In [13], statistical anomaly detection techniques are used to detect rogue nodes that inject false data into VANET. This paper uses the Greenshield traffic model which assumes close vehicles have similar flow, speed and density values. In a decentralized traffic, each vehicle calculates its own value and compares it with average received values until the average value is below the predefined threshold. After that, t-test is applied to these values to determine if the received message comes from an intruder or not.

2.2 Denial of Service Attacks

DoS attacks may cause catastrophic effects to the vehicular traffic, since the decisions of autonomous vehicles may critically depend on the communications between the vehicles and the infrastructure [14]. There are several solution methods proposed for DoS attacks in the literature. In [15], a statistical DoS attack detection model was proposed for the IEEE 802.11 DCF protocol. A Markov chain-based adaptive threshold was used for received Clear-to-Send (CTS) packets by comparing its rate. If the received CTS rate is above the threshold, the source node is labelled as attacker. This method is not suitable for detecting low-rate DDoS attacks. Another DoS attack detector was studied in [16], where MAC layer ACK/SYN packets rates are monitored and compared with a predefined threshold at a centralized node. A packet delivery ratio based jamming attack detection model for VANET was presented in [17], where two different traffic scenarios were considered for performance evaluation.

In [18], authors developed a trust-based framework named TFDD. a hybrid detection model which includes signature-based and anomaly-based detection model, using a data

verification module with honesty weight and quality weight in order to detect attacking vehicles. An unsupervised detection method based on the k-means clustering algorithm was proposed in [19] for jamming attacks in RF-based vehicular communication. In [20], we proposed an anomaly-based IDS for mitigating DDoS attacks, which is significantly enhanced 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 that is studied in the VANET literature. For instance, [21] proposed a Support Vector Machine (SVM) based detection method for clustered VANET. In Sybil attack, attacker identifies itself as multiple nodes. For example, in [22], authors considered detecting sybil attacks using strength analysis for received signals with statistical position verification.

CHAPTER 3: SYSTEM MODEL

3.1 VANET Model

A general two-way traffic flow is considered as shown in Fig. 1. However, the proposed IDSs are not restricted to a specific road type; they can perform well on 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.

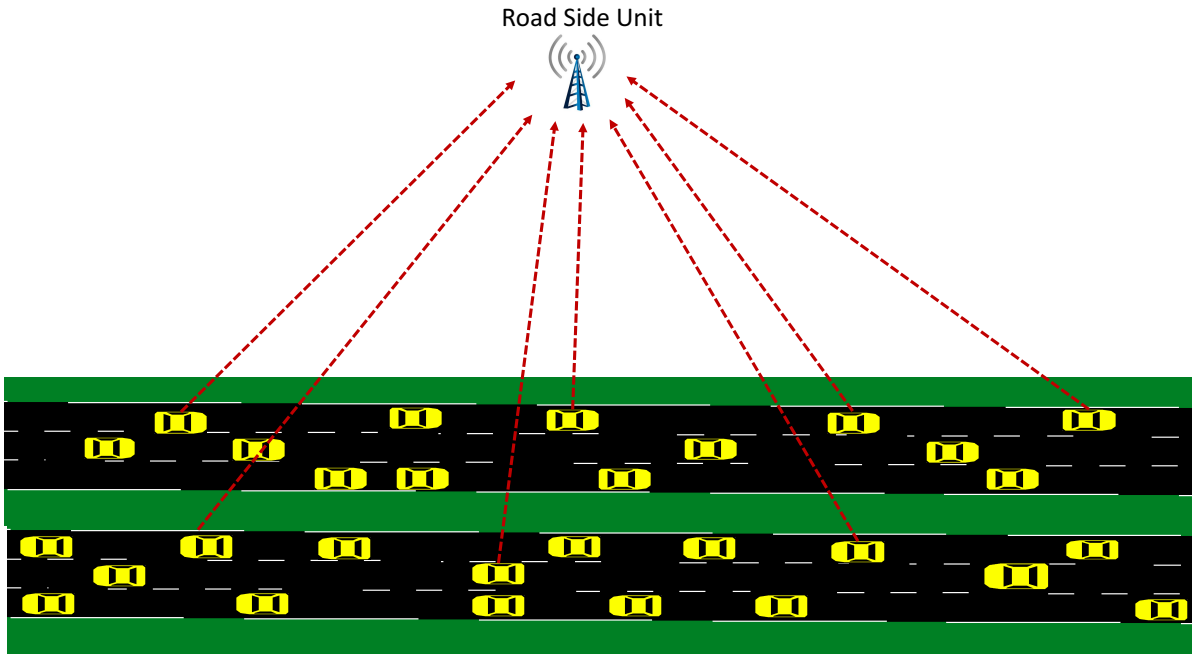

Figure 1: Traffic model for the nominal case where all vehicles broadcast messages and RSU collects these messages.

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, 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 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 the 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.

3.2 Attack Model

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

3.2.1 False Data Injection Attacks

Creating completely a false message or changing some parameters of a message may have a crucial impact on the traffic. Although today's traffic is not dominated yet 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 a flooding of messages may easily overwhelm the attacked RSUs to make the VANET communications unavailable. It is significantly more challenging to detect and mitigate low-rate DDoS attacks than the traditional high-rate 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 low-rate increase in the individual data rates, the greatness in the number of attacking nodes is what makes a low-rate 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 low-rate and high-rate DDoS attacks, as opposed to the traditional data filtering methods.

CHAPTER 4: STATISTICAL INTRUSION DETECTION SYSTEM

In general, anomaly-based 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 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 the significant deviations from the learned nominal statistical model, which is called the semi-supervised setting. Whereas, in the supervised setting, IDS builds also 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 attacks models.

In terms of model parameterization, there are also two types, parametric and nonparametric methods. While parametric methods try to fit certain parametric probability distributions (e.g., Gaussian, Poisson, etc.) to the data, nonparametric methods try to learn statistical patterns from 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: 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 updates a

decision statistic using each observed instance, and decides for anomaly when there is enough statistical evidence for anomaly. Mathematically, their objective is to minimize the expected number of data instances used to detect anomaly while satisfying a constraint on false alarm probability. The challenges in implementing an anomaly-based IDS in VANET 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 is 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 the legitimate users continue receiving regular service. It is known that sequential methods are much more effective in timely detection than outlier detection methods [23].

To address the challenges above we next propose a statistical IDS based on a semi-supervised, nonparametric and sequential anomaly detection technique, called the Online Discrepancy Test (ODIT).

4.1 Attack Detection Using ODIT

ODIT, which was recently proposed in [24], is a computationally efficient real-time anomaly detection algorithm that scales well to large systems [25].

ODIT addresses well the challenges (C1)-(C3) thanks to its semi-supervised, nonparametric and sequential anomaly detection methodology, respectively. Its semi-supervised and nonparametric nature follows an outlier detection method called Geometric Entropy Minimization (GEM) [26]. The decision making procedure of GEM is not sequential. It decides for each observed data instance as nominal or anomalous, which makes it vulnerable to high false alarm rate due to the limitation of statistical significance tests [27]. ODIT successfully combines the semi-supervised and nonparametric features of GEM with the sequential decision making of the Cumulative Sum (CUSUM) change detection algorithm [28]. CUSUM, on the other hand, is a parametric method as it requires the complete knowledge of probability distributions under nominal and anomalous cases. When the assumed distributions exactly match with the actual distributions, CUSUM is known to be minimax optimum in terms of minimizing the average detection delay while satisfying a false alarm constraint [29]. The minimax setting refers to the worst-case scenario with the least favorable anomaly time and observation history. The practical version of CUSUM, called Generalized CUSUM (G-CUSUM), in a supervised fashion, estimates the parameters of assumed nominal and anomalous probability distributions from training data, i.e., fits the assumed distributions to the available data. Due its dependency on anomalous training data and parametric models G-CUSUM cannot address the challenges (C1) and (C2), respectively.

Consider that each data instance $i \in R^d$ is a d-dimensional real-valued vector representing the observed d data dimensions $\{x_i^1, \ldots\ldots, x_i^d\}$ depending on the application. The specific definition of data dimensions is given in Sections 4.3 and 4.4 for FDI and DDoS attacks, respectively. In ODIT, there is no 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, e.g., using mean and standard deviation, or upper and lower bounds, or some practical bounds such as *5th* and *95the* percentiles. Normalization is needed to deal with the heterogeneity among data dimensions.

In the training phase of ODIT, firstly training data $\mathcal{X}_N$ is randomly partitioned into two sets $\mathcal{X}_{N1}$ and $\mathcal{X}_{N2}$, where *N1+N2=N*, for computational purposes as in the Bipartite GEM algorithm [30]. Then, for each data point in $\mathcal{X}_{N1}$, k nearest neighbors (*kNN*) in $\mathcal{X}_{N2}$ in terms of Euclidean distance are found. For each point i in $\mathcal{X}_{N1}$ the total distance *Li* 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 $\mathcal{X}_{N1}$ to its *jth* nearest neighbor in $\mathcal{X}_{N2}$. 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 method.

Next, for a significance level α, for which a typical choice is *0.05*, the $(1-\alpha)$ th percentile L_M of $\{L_i : i = 1 \ldots . N_1\}$ values is found, where $M = [N_1(1-\alpha)]$. The L_M value is later used as a baseline in the test to evaluate the anomaly evidence in the test instances. During the training phase, actually an Euclidean kNN graph is formed between $(1-\alpha)\%$ of the points in $\mathcal{X}_{N1}$ with the smallest L_i values and their neihbors in $\mathcal{X}_{N2}$, as illustrated in Fig. 2. As we will show next, in

the test phase of ODIT, we actually evaluate how far/close a test instance is in becoming a vertex in this graph if it were to be included in $\mathcal{X}_{N1}$. From another perspective, $(1-\alpha)\%$ of the points with the smallest L_i values in $\mathcal{X}_{N1}$ is an estimate of the "minimum volume set" which is the most compact set that has at least $(1-\alpha)$ probability [26], and in the test phase, we measure how far/close a test instance is to be included in this most compact set.

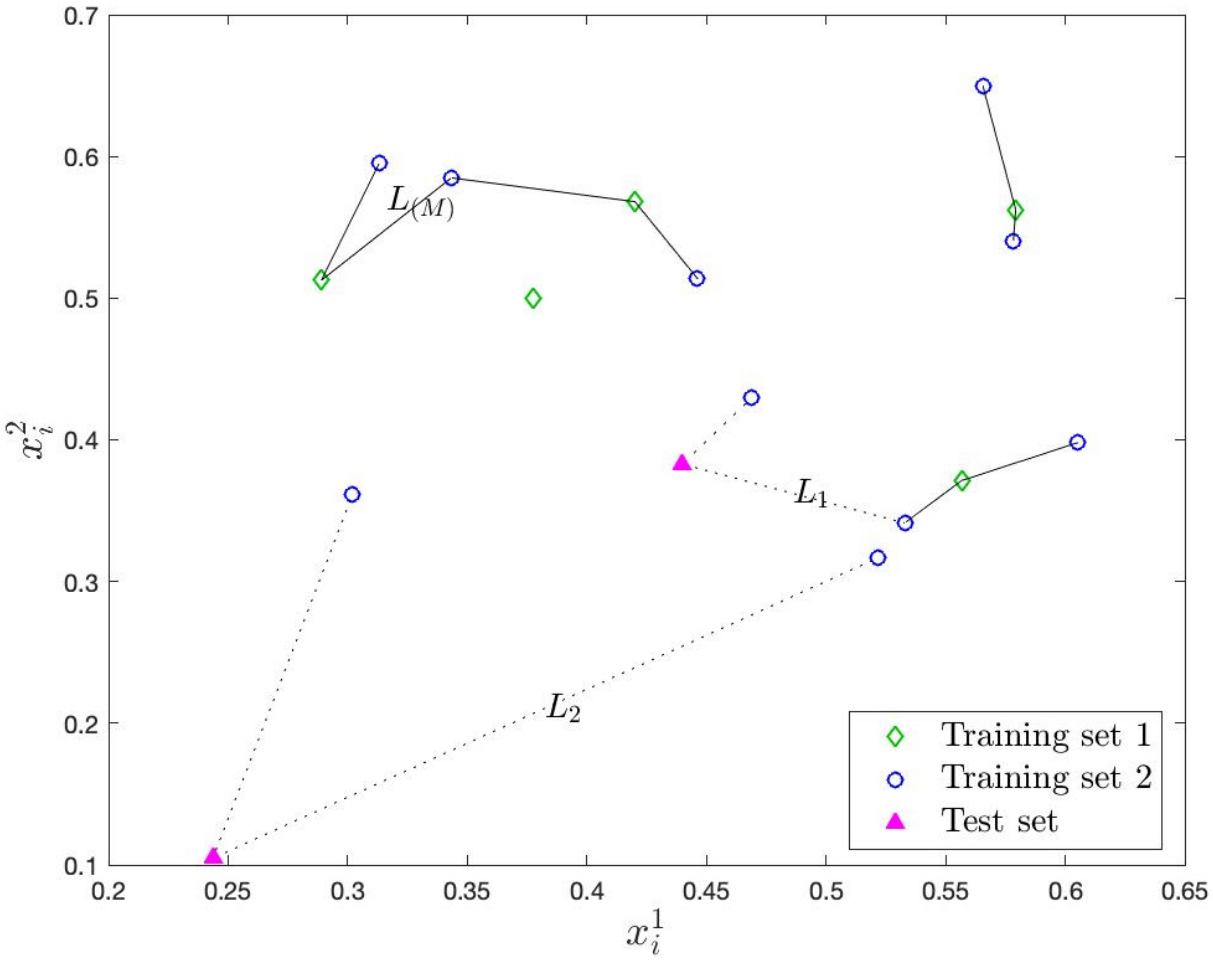

Figure 2: Proposed detection procedure based on ODIT with $N_1 = 5, N_2 = 10, M = 4, k = 2, s = 1, \gamma = 1$. $L_1 - L_M$ and $L_1 - L_M$ are used to update the test statistic s_t and raise an alarm at time T as shown in (2)-(4). Training and test points are generated from a bivariate normal distribution with independent components, 0.5 mean and 0.1 standard deviation.

In the test phase, to evaluate the anomaly evidence in a newly observed instance x_t at time t, we compute how small/big the total distance L_t of 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 as in (1), and the anomaly evidence

$$D_t = L_t - L_{(M)}, \tag{2}$$

which asymptotically behaves like the log-likelihood ratio between a uniform distribution and the nominal distribution [24]. Note that the anomaly evidence provided by D_t can be positive or negative. Unlike the outlier detection methods such as GEM, ODIT does not decide for each instance, but rather accumulates the anomaly evidences over time by updating its decision statistic as

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

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

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

The detection threshold h manifests a trade-off between minimizing detection delay and minimizing false alarm rate. For example, higher h decreases the false alarm probability at the expense of larger average detection delay, and vice versa for lower h. In practice, h can be set such that a desired false alarm probability is satisfied. The selection of other parameters also indirectly affect this fundamental trade-off of quick and accurate detection. Particularly, for bigger/smaller number of neighbors k, ODIT becomes more/less robust to noise (i.e., nominal outliers), but at the same time the 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 α does not play a central role in

ODIT, as opposed to GEM, in which α 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 ODIT, the affect of the α 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 α, and then h is chosen to satisfy a desired false alarm rate.

4.2 Attack Localization Using ODIT

Detecting an attack is in general not the final task for successful mitigation. Especially for low-rate 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. To this end, we next propose a statistical anomaly localization technique for ODIT to identify the anomalous data dimensions.

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 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

$$L_t = \sum_{n=1}^{d} \ell_t^n \text{ where } \ell_t^n = \sum_{j=k-s+1}^{k} (x_t^n - y_j^n)^2, \tag{5}$$

and x_t^n and y_j^n are the nth dimensions of the data instancex_t and its jth nearest neighbor y_j. Note that ℓ_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 ℓ_t^n right before the detection time T. We determine the number of recent ℓ_t^n values contributing to alarm by first identifying the last time instance q 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

$$\bar{\ell}^n = (T-q)^{-1} \sum_{t=q+1}^{T} \ell_t^n, \tag{6}$$

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 λ controls the trade-off between false positive and true positive rates, as shown in Fig. 14. It is typically selected to satisfy a constraint on the false positive rate [31].

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

4.3 Proposed IDS for FDI Attack

In this section, we propose an IDS based on ODIT for FDI attack. In the proposed IDS, each RSU runs a separate ODIT detector for each vehicle that it receives messages from. In particular, an RSU starts to monitor a vehicle by updating a decision statistic s_t (see (3)) for it when the vehicle enters its range until either the vehicle exits the range or an anomaly in the message content is detected. The data instance x_t consists of three components, namely the speed, position, direction of the vehicle. The nominal training data X_N is obtained through historical observations in the range of RSU. If the range is composed of heterogeneous road segments with different speed and direction baselines, then multiple training sets, and accordingly multiple L_M obtained for such road segments. Depending on the vehicle's position the test instance x_t is then

Algorithm 1 Proposed detection & 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 $x_i \, \epsilon \, \mathcal{X}_{N_1}$ as in (1)
Find $L_{(M)}$ by selecting the Mth smallest L_i
Test phase
while $s_t < h$ **do**
    $t \leftarrow t + 1$
    Get new data x_t and compute $D_t = L_t - L_{(M)}$
    $s_t = \max\{s_{t-1} + D_t, 0\}$
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 (6)
    if $\bar{\ell}^n \geq \lambda$ **then**
        Declare dimension n as attacking
    end if
end for

compared with the corresponding road segment's baseline L_M value. Algorithm 1 is used to detect and localize FDI attacks. Once a vehicle is detected as anomalous, RSU informs the other vehicles and RSUs. Depending on the system operator's choice, either the identified anomalous dimensions or the complete messages from the detected vehicle are ignored. The flowchart of the proposed IDS is given in Fig. 3.

4.4 Proposed IDS for DDoS Attack

A straightforward approach to DDoS detection is through comparing the incoming message rate (i.e., number of messages per unit time) from each vehicle with a threshold. Although this method can stop brute-force attacks in which attackers transmit burst of data messages at a high

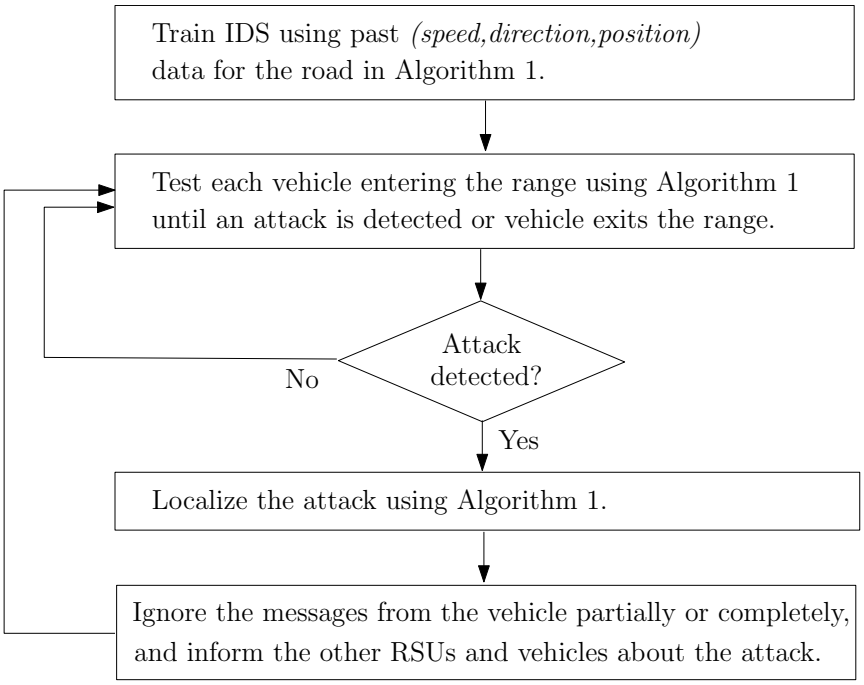

Figure 3: Flowchart of the proposed IDS for FDI attacks.

rate, it would not be effective against stealth low-rate attacks in which each attacker transmits messages at a close-to-nominal rate, yet synchronously they can overwhelm the RSU. Admittedly, the straightforward approach that compares the total data rate from all vehicles with a threshold can easily detect DDoS attack (either high-rate or low-rate); however, it cannot identify the attackers to stop the attack. To this end, we propose a statistical IDS that jointly monitors vehicles through ODIT. Since the number of vehicles in the range of an RSU varies over time, for joint (i.e., multivariate) monitoring of data traffic, we consider total message rates in a number of predetermined road segments as the input data to the ODIT algorithm, $x_t = [x_t^1, \ldots\ldots, x_t^n]$ where x_t^n is the message rate from road segment n at time interval t (see Fig. 5). When a DDoS attack is detected and localized using Algorithm 1, the data traffic from the identified road segments are blocked to mitigate the attack. 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 Fig. 4.

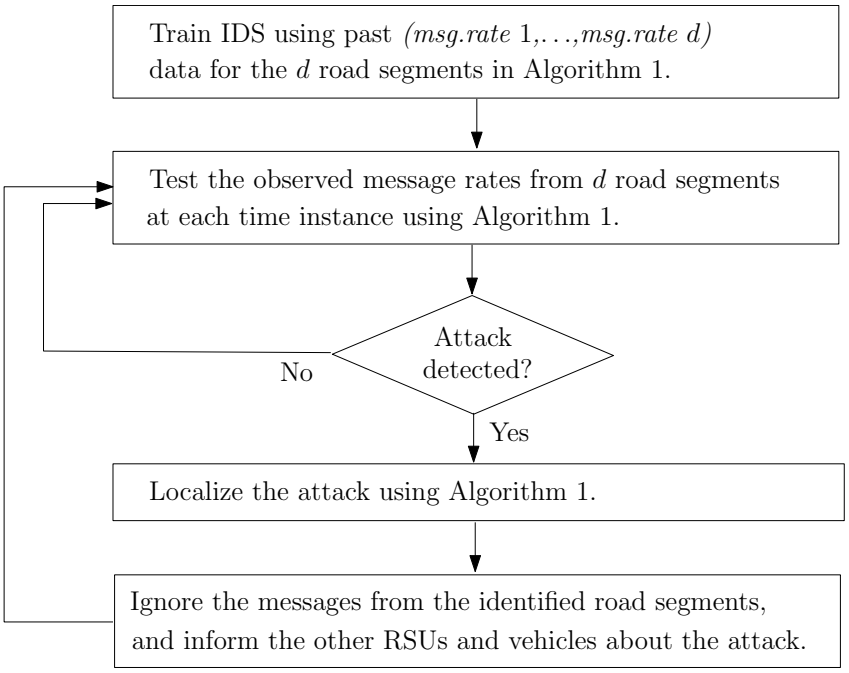

Figure 4: Flowchart of the proposed IDS for DDoS attacks.

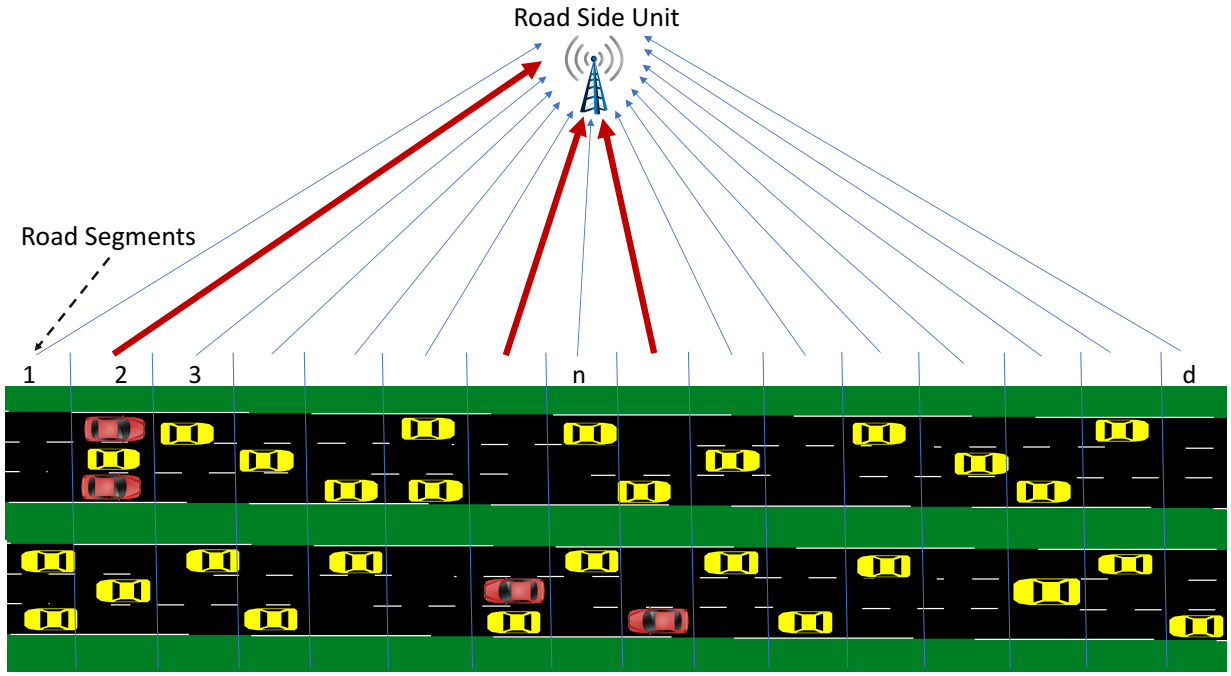

Figure 5: DDoS attack model where red cars are attackers and thick red lines denote the increased data rates.

CHAPTER 5: PERFORMANCE EVALUATION

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

5.1 Detection Results for FDI Attack

5.1.1 Experiment Setup

We use the Warrigal dataset, collected by the University of Sydney in an industrial area over a period of three months with 1 Hz resolution [32]. Each message in the dataset consists of position, speed and direction information. Position information is given in three dimensions as easting, northing and altitude in meters. Speed and direction values are provided in meter/second and degrees, respectively. The histograms of training data for position (easting), speed and direction are shown in Fig. 6. 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 is collected from a few km road range, where RSU is assumed to be located at the center. The proposed IDS is implemented at the RSU following the flowchart presented in Fig. 3.

In order to generate FDI attack scenarios, we separately injected anomalous data in each dimension. In each scenario, anomalous data is injected into one of the data dimensions of a randomly selected set of vehicles (i.e., attacking vehicles). Anomaly rates for position and direction are *30%* and *40%* of the nominal values, respectively. After anomaly injection, the falsified speed 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 Fig. 6. For each test, anomaly is inserted in one of the message dimensions for only 20 seconds.

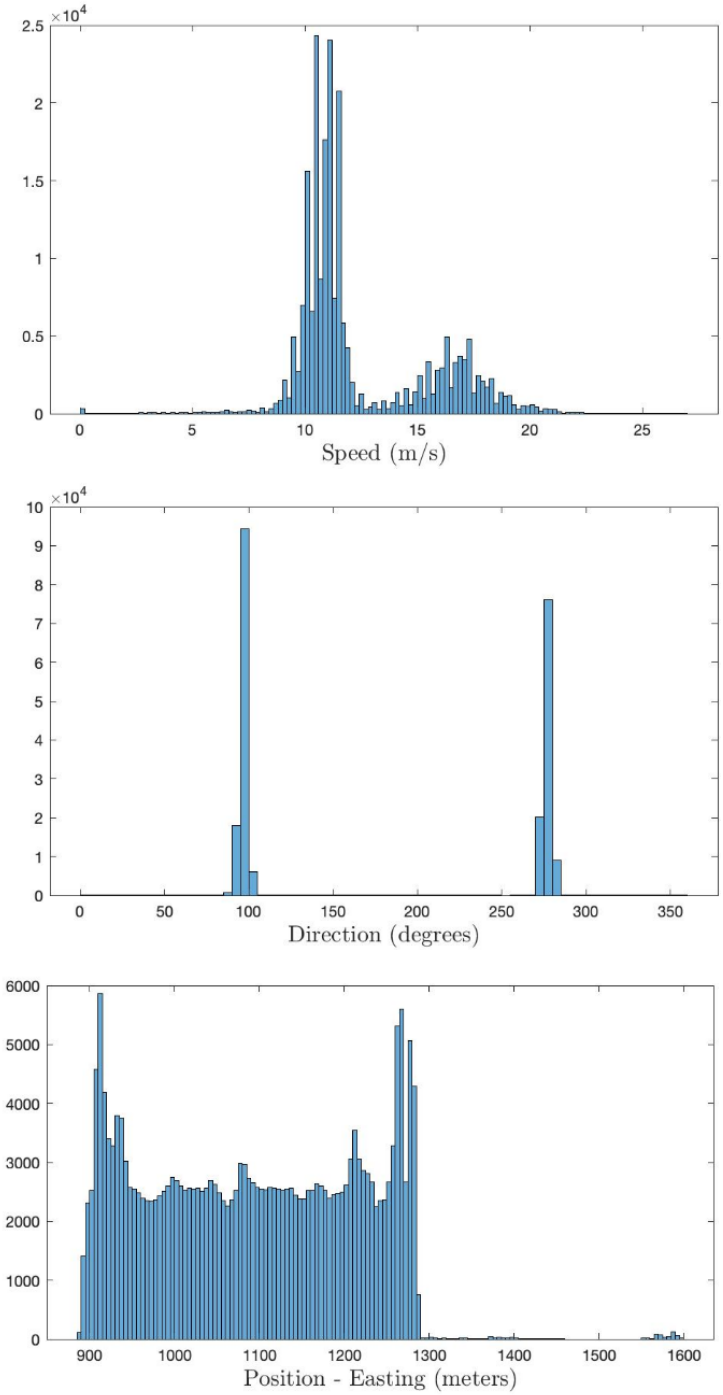

Figure 6: The heterogeneous probability distributions of message contents in the Warrigal dataset. Histograms are obtained from the training set.

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 Fig. 6 is somehow close to two gaussian sub-distributions within overall one distribution, which is named as a Gaussian Mixture Model (GMM), G-CUSUM assumes a GMM type of probability distributions for both nominal and anomaly data. Three FDI attack scenarios are investigated for anomalies in the speed, position, and direction data, whose results are given in Fig. 7. Middle figure in Fig 7 shows the results for the case when anomaly is in easting dimension of position in which similar results are observed with northing dimension of position as well. The data-driven nature of ODIT enables much quicker detection while satisfying the same false alarm rates compared to G-CUSUM. ODIT 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.

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 [13], ELIDV [10], and DCMD [9]. These systems run on each vehicle where each received message content is examined with a voting scheme. A main performance difference between such models and ODIT is that while the detection accuracy for these systems decreases with increasing number of anomalous vehicles due to the in-

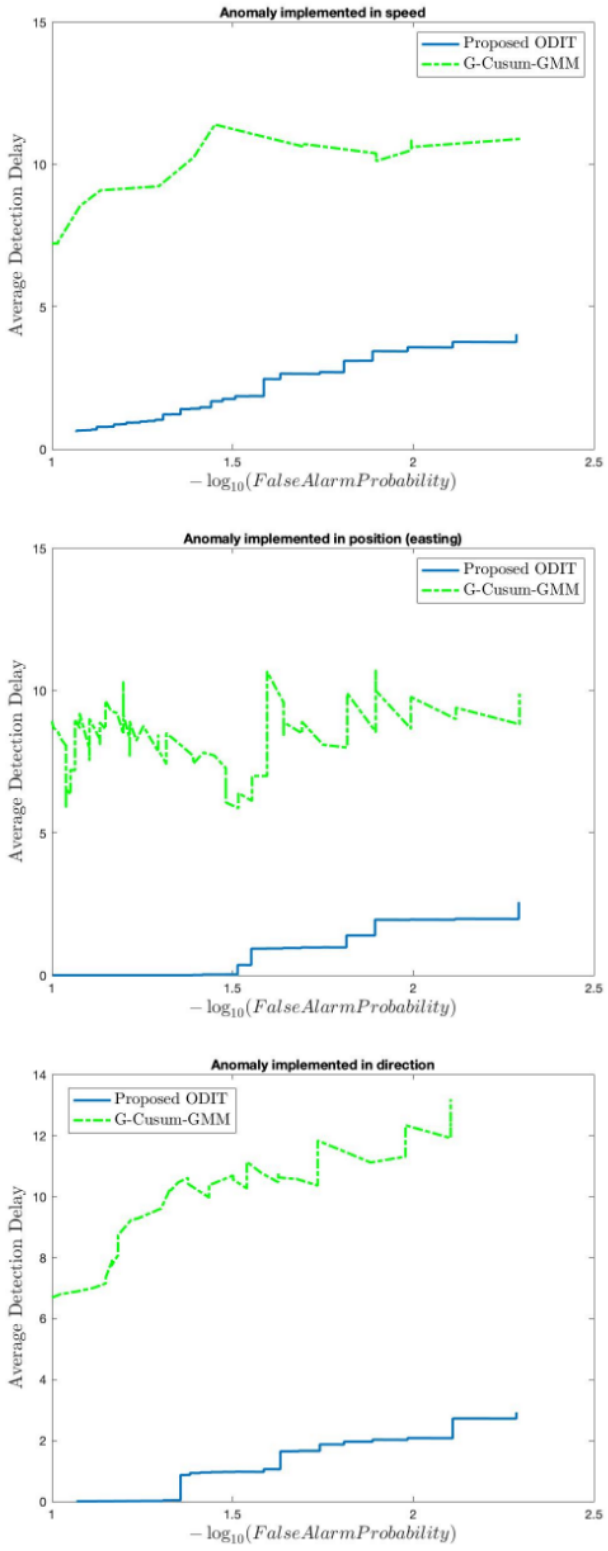

Figure 7: Comparison in terms of quick and accurate detection under different FDI attack scenarios between the proposed detector and an idealized version of the state-of-the-art sequential detector (G-CUSUM) which exactly knows the attack magnitudes.

herent rules of voting, that of ODIT is not affected since each vehicle is monitored at the RSU. This fact is illustrated in Fig. 8 in terms of true positive rate and false positive rate, respectively, considering the anomalous speed scenario. The proposed ODIT detector achieves *100%* detection (true positive rate) and *0%* false alarm (false positive rate) 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. For ODIT, successful detection (true positive) is defined as raising an anomaly alarm within the first *12* seconds after the attack starts.

5.2 Detection Results for DDoS Attack

5.2.1 Experiment Setup

In this section, we evaluate the performance of proposed IDS for low-rate DDoS attacks targeting the availability of VANET communications. As shown in Fig. 5, we split an RSU range into equal road segments. Total number of received message from a road segment in a time interval is considered as the message rate observations, which mainly depend on the number of vehicles and speed of vehicles. For example, if traffic flow decreases, leading to a rise in the number of vehicles on the road, the message rate increases on the road segments.

For the simulation study, we use three framework together: OMNET++ [33], SUMO [34], and Veins [35]. 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 [36], but since our model does not specify any communication protocol, our DDoS detection algorithm can be used with other protocols as well.

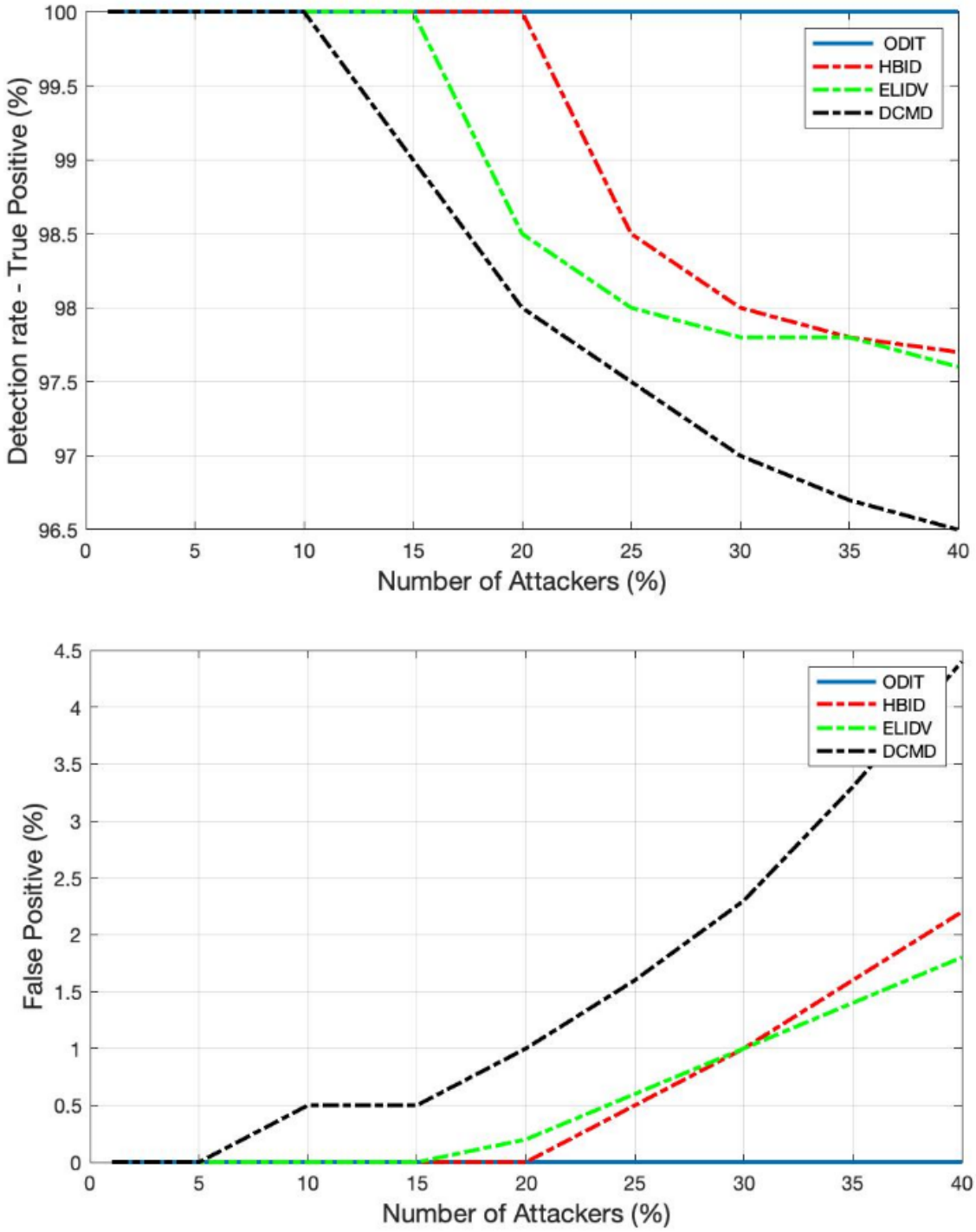

Figure 8: Comparison considering FDI attack in speed values between the proposed ODIT detector and several voting-based detectors from the literature.

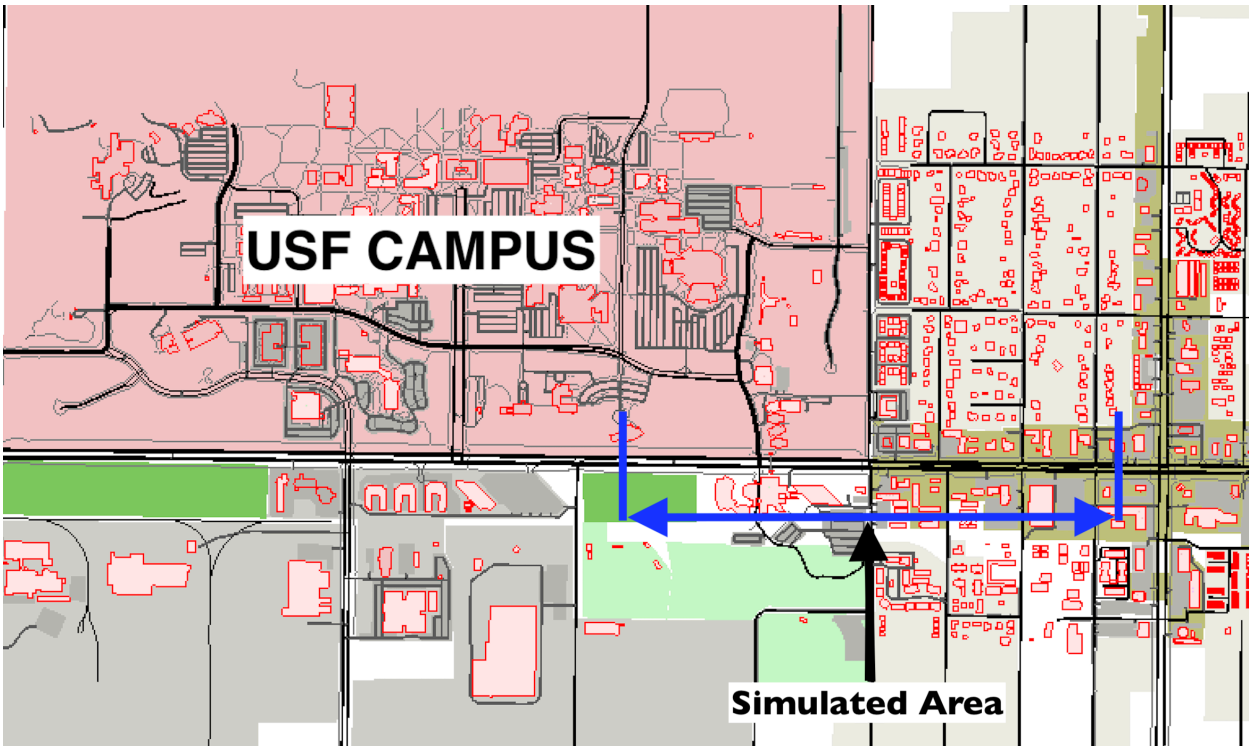

Figure 9: Simulation map showing Fowler Ave.

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) in Tampa (See Fig. 9). Selected road section is partitioned into 20 segments with 50 meters width for each road segment. In order to have a realistic dataset, there is no restriction on vehicular movements where all vehicles follow their randomly generated routes, i.e., they can join or leave the main road at any intersection. Average number of vehicles in the simulation area is 250.

With the given simulation parameters in Table 5.1, 4 hours of traffic is observed for learning the training baseline and 33.3 hours of traffic is observed for the test purposes. After saving all the log files, data rates for each road segment are calculated on MATLAB, and 600 test trials of 200-second duration are obtained. We generated anomaly data in MATLAB from 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 181st second to 200th second.

Table 5.1: Simulation Parameters

Simulation Area	9000 x 5000 m^2
Simulation Time (Each Trial)	200s
Number of Trials	600
Average Number of Vehicle	250
Traffic Generation	Random
Route Generation	Random
Network Protocol	IEEE 802.11p
Beacon Rate	1s
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., [37], and the data filtering method, e.g., [16]. 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 Fig. 10 and Fig. 11, it is seen that the observations from two road segments, to which anomaly is added, follow different distributions. While the distribution of one road segment is similar to negative binomial (Fig. 10), which is indeed a Poisson distribution with conjugate prior (i.e., Gamma distribution) on the rate

parameter, the distribution of other road segment is similar to Gaussian (Fig. 11). 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, Fig. 12 and Fig. 13 show that the proposed IDS outperforms the G-CUSUM approach and the data filtering approach in terms of quick and accurate detection. In particular, the proposed IDS achieves 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 Figs. 12 and 13). 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 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 Figs. 12 and 13, even the ideal G-CUSUM which exactly knows the attack magnitude suffers from the deviations of the observed data from the assumed probability distributions. Furthermore, G-CUSUM inevitably follows a univariate approach by assuming independence between road segments [38] since it does not know which road segments will include anomaly. The multivariate nature of the proposed ODIT detector also facilitates its superior performance.

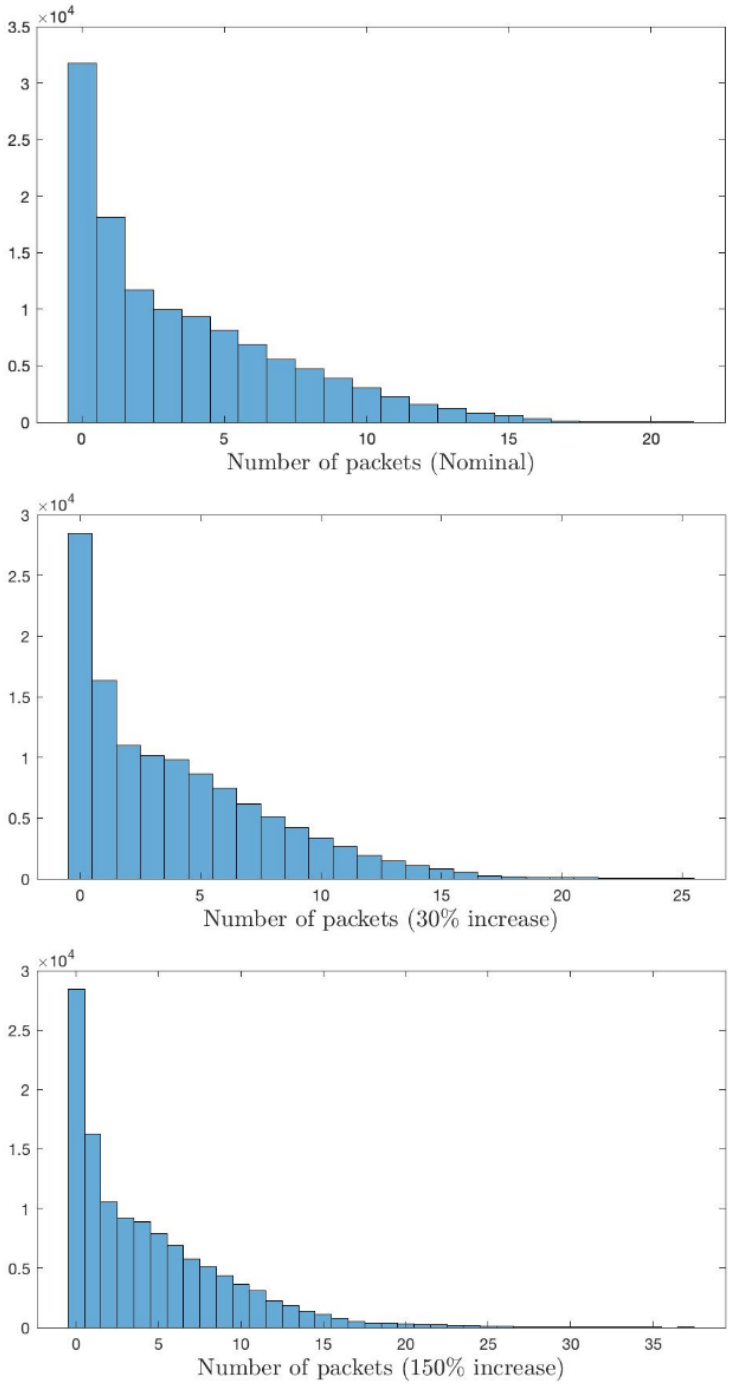

Figure 10: Histogram of number of packets for a road segment. First histogram represents the distribution of nominal data, whereas second and third represent attack cases with an average increase that is 0.3 and 1.5 times the baseline, respectively. Nominal and attack distributions are close to negative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

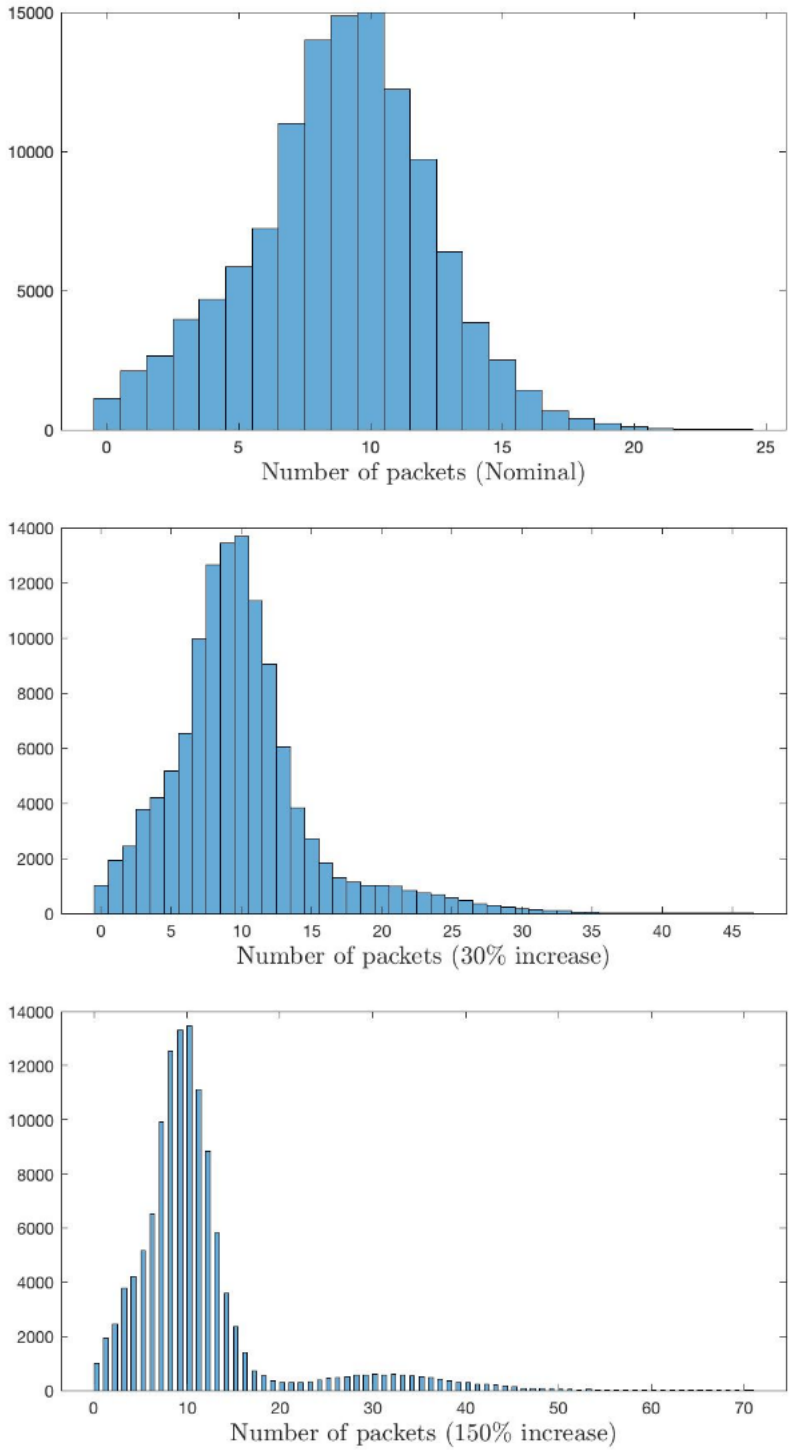

Figure 11: Histogram of number of packets for a road segment. First histogram represents the distribution of nominal data, whereas second and third represent attack cases an average increase that is 0.3 and 1.5 times the baseline, respectively. Nominal and attack distributions are close to normal distribution with extended tails under attacks.

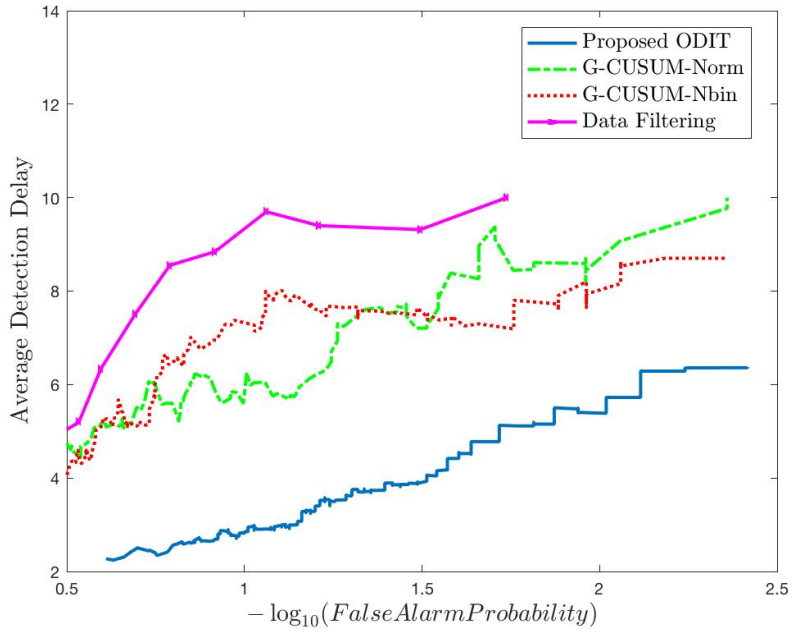

Figure 12: Comparison in terms of quick and accurate detection for an average DDoS attack magnitude of 0.3 times the nominal mean data rate between the proposed method, two idealized G-CUSUM variants which exactly know the attack magnitude, and the data filtering method.

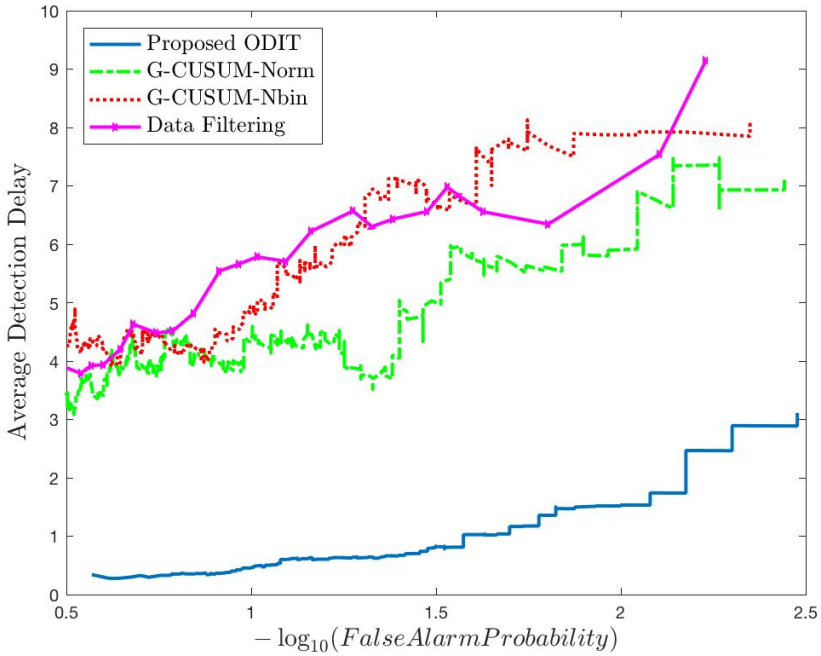

Figure 13: Comparison in terms of quick and accurate detection for an average DDoS attack magnitude of 1.5 times the nominal mean data rate between the proposed method, two idealized G-CUSUM variants which exactly know the attack magnitude, and the data filtering method.

5.3 Localization Results

We next evaluate the attack localization performance of the proposed IDS using the receiver operating characteristic (ROC) curves, which presents the achieved true positive rates while the algorithm satisfies different levels of false positive constraints. Firstly, we consider the identification of attacking vehicles in the FDI attack scenario (anomalous speed case). Since in this case the proposed ODIT 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 ODIT alarms for 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 alarm for non-attacking vehicles and 100% correct detection of attacking vehicles with a maximum delay of 12 seconds (First figure in Fig. 14). We next consider the identification of anomalous data dimension using the localization strategy given in (6) and summarized by Algorithm 1. Second figure in Fig. 14 displays the perfect detection of the anomalous speed data while satisfying zero false alarm in all test trials.

Finally, the identification of road segments in the DDoS attack scenario using Algorithm 1 is considered. As demonstrated by third figure in Fig. 14, 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%).

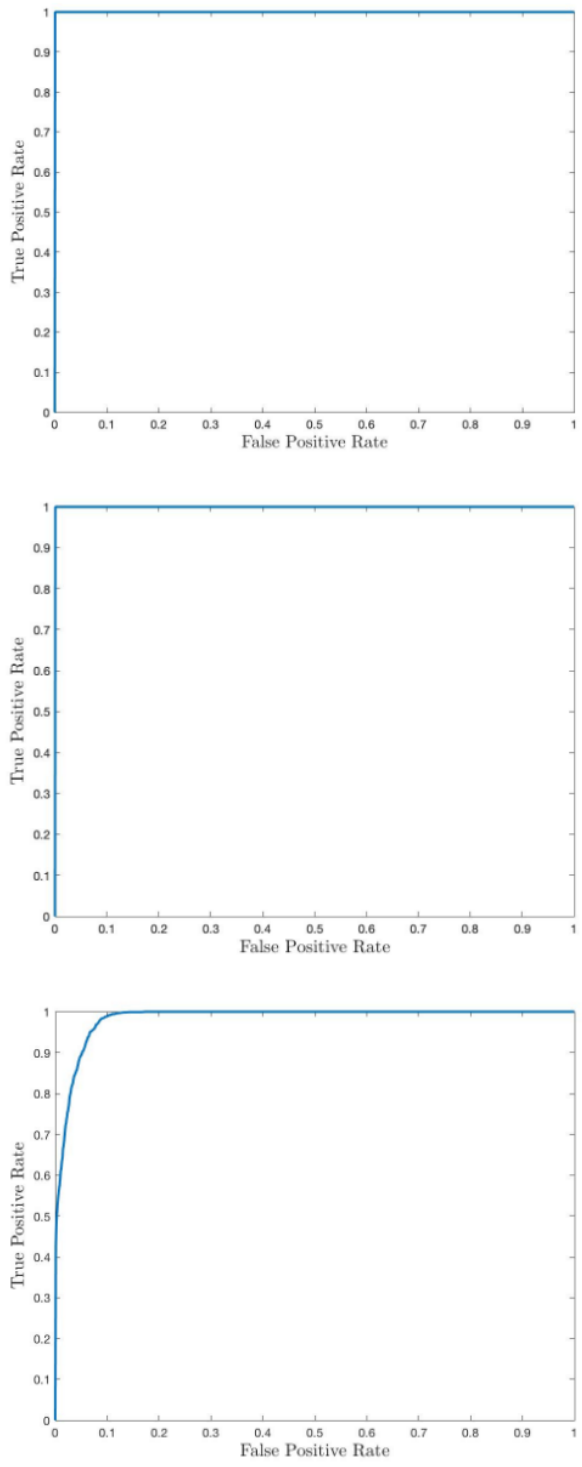

Figure 14: ROC curves for ODIT's anomaly localization performance. First figure is for identification of anomalous vehicles in FDI attack to speed data. The second one is for identification of anomalous data in FDI attack to speed data. The last one is for identification of anomalous road segments in DDoS attack.

CHAPTER 6: CONCLUSION

We proposed a statistical nonparametric intrusion detection system (IDS) for online detection of false data injection (FDI) attacks and distributed denial-of-service (DDoS) attacks. The proposed system runs at road side unit (RSU) monitoring the 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 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 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. Experiment 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. As a future work, we plan to extend the proposed IDS to other attack types.

REFERENCES

[1] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti. Vanet securitychallenges and solutions: A survey. Vehicular Communications, 7:7–20, 2017.

[2] Mani Amoozadeh, Arun Raghuramu, Chen-Nee Chuah, Dipak Ghosal, H Michael Zhang, Jeff Rowe, and Karl Levitt. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Communications Magazine, 53(6):126–132, 2015.

[3] Seyed Ahmad Soleymani, Abdul Hanan Abdullah, Wan Haslina Hassan, Mohammad HosseinAnisi, Shidrokh Goudarzi, Mir Ali Rezazadeh Baee, and Satria Mandala. Trust management in vehicular ad hoc network: a systematic review. EURASIP Journal on Wireless Communications and Networking, 2015(1):146, 2015.

[4] Uzma Khan, Shikha Agrawal, and Sanjay Silakari. A detailed survey on misbehavior node detection techniques in vehicular ad hoc networks. In Information systems design and intelligent applications, pages 11–19. Springer, 2015.

[5] Changwang Zhang, Zhiping Cai, Weifeng Chen, Xiapu Luo, and Jianping Yin. Flow level detection and filtering of low-rate ddos. Computer Networks, 56(15):3417–3431, 2012.

[6] Zhaomin Chen, Chai Kiat Yeo, Bu Sung Lee, and Chiew Tong Lau. Power spectrum entropy based detection and mitigation of low-rate dos attacks. Computer Networks, 136:80–94, 2018.

[7] J. Petit and S. E. Shladover. Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent Transportation Systems, 16(2):546–556, April 2015.

[8] Philipp Wex, Jochen Breuer, Albert Held, Tim Leinmuller, and Luca Delgrossi. Trust issues for vehicular ad hoc networks. In Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, pages 2800–2804. IEEE, 2008.

[9] Sushmita Ruj, Marcos A Cavenaghi, Zhen Huang, Amiya Nayak, and Ivan Stojmenovic. On data-centric misbehavior detection in vanets. In Vehicular technology conference (VTC Fall), 2011 IEEE, pages 1–5. IEEE, 2011.

[10] Hichem Sedjelmaci, Sidi Mohammed Senouci, and Mosa Ali Abu-Rgheff. An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks. IEEE Internet of things journal, 1(6):570–577, 2014.

[11] Hichem Sedjelmaci, Sidi Mohammed Senouci, and Tarek Bouali. Predict and prevent frommisbehaving intruders in heterogeneous vehicular networks. Vehicular Communications, 10:74–83, 2017.

[12] Rens W Van der Heijden, Frank Kargl, Osama MF Abu-Sharkh, et al. Enhanced positionverification for vanets using subjective logic. In Vehicular Technology Conference (VTCFall), 2016 IEEE 84th, pages 1–7. IEEE, 2016.

[13] Kamran Zaidi, Milos B Milojevic, Veselin Rakocevic, Arumugam Nallanathan, and Muttukrishnan Rajarajan. Host-based intrusion detection for vanets: a statistical approach to rogue node detection. IEEE transactions on vehicular technology, 65(8):6703–6714, 2016.

[14] S. Parkinson, P. Ward, K. Wilson, and J. Miller. Cyber threats facing autonomous and connected vehicles: Future challenges. IEEE Transactions on Intelligent Transportation Systems, 18(11):2898–2915, Nov 2017.

[15] Joseph Soryal and Tarek Saadawi. Dos attack detection in internet-connected vehicles. In Connected Vehicles and Expo (ICCVE), 2013 International Conference on, pages 7–13. IEEE, 2013.

[16] Karan Verma, Halabi Hasbullah, and Ashok Kumar. Prevention of dos attacks in vanet. Wireless personal communications, 73(1):95–126, 2013.

[17] Lynda Mokdad, Jalel Ben-Othman, and Anh Tuan Nguyen. Djavan: Detecting jamming attacks in vehicle ad hoc networks. Performance Evaluation, 87:47–59, 2015.

[18] Chaker Abdelaziz Kerrache, Nasreddine Lagraa, Carlos T Calafate, and Abderrahmane Lakas.Tfdd: A trust-based framework for reliable data delivery and dos defense in vanets. Vehicular Communications, 9:254–267, 2017.

[19] Dimitrios Karagiannis and Antonios Argyriou. Jamming attack detection in a pair of rf communicating vehicles using unsupervised machine learning. Vehicular Communications, 13:56–63, 2018.

[20] Ammar Haydari and Yasin Yilmaz. Real-time detection and mitigation of ddos attacks intelligent transportation systems. In 2018 21st International Conference on Intelligent Transportation Systems (ITSC), pages 157–163. IEEE, 2018.

[21] Omar Abdel Wahab, Azzam Mourad, Hadi Otrok, and Jamal Bentahar. Ceap: Svm-based intelligent detection model for clustered vehicular ad hoc networks. Expert Systems with Applications, 50:40–54, 2016.

[22] Bo Yu, Cheng-Zhong Xu, and Bin Xiao. Detecting sybil attacks in vanets. Journal of Parallel and Distributed Computing, 73(6):746–756, 2013.

[23] H Vincent Poor and Olympia Hadjiliadis. Quickest detection, volume 40. Cambridge University Press Cambridge, 2009.

[24] Yasin Yilmaz. Online nonparametric anomaly detection based on geometric entropy minimization. In Information Theory (ISIT), 2017 IEEE International Symposium on, pages 3010–3014. IEEE, 2017.

[25] Yasin Yilmaz and Suleyman Uludag. Mitigating iot-based cyberattacks on the smart grid. In Machine Learning and Applications (ICMLA), 2017 16th IEEE International Conference on, pages 517–522. IEEE, 2017.

[26] Alfred O Hero. Geometric entropy minimization (gem) for anomaly detection and localization. In Advances in Neural Information Processing Systems, pages 585–592, 2007.

[27] Monya Baker. Statisticians issue warning over misuse of p values. Nature News, 531(7593):151, 2016.

[28] Ewan S Page. Continuous inspection schemes. Biometrika, 41(1/2):100–115, 1954.

[29] George V Moustakides et al. Optimal stopping times for detecting changes in distributions. The Annals of Statistics, 14(4):1379–1387, 1986.

[30] Kumar Sricharan and Alfred O Hero. Efficient anomaly detection using bipartite k-nn graphs. In Advances in Neural Information Processing Systems, pages 478–486, 2011.

[31] H Vincent Poor. An introduction to signal detection and estimation. Springer Science Business Media, 2013.

[32] James Ward, Stewart Worrall, Gabriel Agamennoni, and Eduardo Nebot. The warrigal dataset: Multi-vehicle trajectories and v2v communications. IEEE Intelligent Transportation Systems Magazine, 6(3):109–117, 2014.

[33] Andr´as Varga and Rudolf Hornig. 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, page 60. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

[34] Michael Behrisch, Laura Bieker, Jakob Erdmann, and Daniel Krajzewicz. Sumo–simulation of urban mobility: an overview. In Proceedings of SIMUL 2011, The Third International Conference on Advances in System Simulation. ThinkMind, 2011.

[35] Christoph Sommer, Reinhard German, and Falko Dressler. Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis. IEEE Transactions on Mobile Computing, 10(1):3–15, January 2011.

[36] Daniel Jiang and Luca Delgrossi. Ieee 802.11 p: Towards an international standard for wireless access in vehicular environments. In Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, pages 2036–2040. IEEE, 2008.

[37] Yinghua Guo and Ivan Lee. Forensic analysis of dos attack traffic in manet. In Network and System Security (NSS), 2010 4th International Conference on, pages 293–298. IEEE, 2010.

[38] Yajun Mei. Efficient scalable schemes for monitoring a large number of data streams. Biometrika, 97(2):419–433, 2010.