Trust-based Adversary Detection in Edge Computing Assisted Vehicular Networks

Nalam Venkata Abhishek and Teng Joon Lim

***Abstract*—Low-latency requirements of vehicular networks can be met by installing mobile edge hosts that implement mobile edge computing in the roadside units (RSUs). Adversaries can, however, compromise these RSUs and use them to launch cyber attacks. In this paper, we consider an adversary that selectively drops packets or selectively corrupts packets between the RSU and passing vehicles. Such strategies would lead to a higher number of re-transmissions and thereby increase the latency of the network, which in turn impacts critical delay-sensitive applications like collision avoidance, emergency vehicle warning, etc. We propose to use trust-based detection systems to detect such an adversary. Each vehicle transmits its uplink and downlink trust values about every RSU it has interacted with. These trust values are relayed to the RSU gateway, where the decision will be made, via the next RSU encountered by a vehicle. At regular intervals, the gateway aggregates the uplink and downlink trust values obtained from multiple vehicles. It compares them against their respective thresholds to classify the RSU as benign or malicious. We also consider the presence of malicious vehicles trying to deceive the detection system by reporting false trust values. A detection mechanism is proposed to detect such vehicles. Simulation results generated using MATLAB are presented to demonstrate the performance of the proposed detection mechanisms and the impact of the adversary's parameters on the detection systems.**

***Index Terms*—Malicious road side unit, least squares, trust, vehicular networks.**

I. INTRODUCTION

VEHICULAR networks (VNETs) are fast emerging and prominent technologies for realizing safe and efficient transportation systems. There are mainly two types of channels equipped in VNETS; vehicle-to-vehicle communication (V2VC) and vehicle-to-roadside unit (or infrastructure) communication (V2IC). With V2VC and V2IC, real-time information exchange among vehicles and between vehicles and central control systems are enabled, which in turn enables a host of safety, navigational, and infotainment enhancements. Among these, road safety and traffic efficiency applications have the strictest requirements in terms of data quality, latency, and communication reliability. Time-sensitive applications must operate with a communication latency of less than 50 ms [1]. To ensure reliability and low latency, mobile edge computing (MEC) is a potential solution [2], [3] as it provides computing services in close proximity to vehicles that need them. In VNETS, MEC can be realized by installing mobile edge hosts (MEHs) on the roadside units (RSUs) or locating the MEHs physically close to the RSUs. Vehicles offload their resource-intensive operations onto these MEHs and run applications on multiple platforms. Many factors influence MEC server deployment, including scalability, physical deployment limits, and/or performance standards (e.g., delay). There have been limited work in the literature that address these issues [4]. Mostly the authors have focused on finding a trade-off between installation costs and QoS measured in terms of latency.

VNETs are vulnerable to various attacks that compromise availability, confidentiality, integrity, and authenticity. Researchers have proposed many methods to overcome attacks like Sybil attack, Bogus information attack, wormhole, denial of service (DoS), etc. [5], [6] that originate from compromised vehicles and primarily affect V2VC. All these attacks can be countered with high reliability using the methods previously proposed [7], [8]. Therefore, attacks affecting V2VC are not addressed in this paper.

The attacks on the wireless link between a vehicle and an RSU in a VNET are similar to the attacks on the link between a Mobile and a base station in mobile networks. Attacks that affect such links like jamming, eavesdropping, rogue base stations, etc., have already been addressed. However, RSUs are not as secure as base stations in mobile networks. Edge data centers generally include legacy edge devices or are composed of microservers with limited connectivity. Therefore, authentication protocols may not be easily implemented and it may then be easier for an adversary to launch attacks. Adversaries, in such cases, can launch attacks like privacy leakage, physical damage, rogue data center, channel degradation, service manipulation, etc.

A. Related Work

This section presents those attacks that can affect V2IC and are well investigated in the literature. There are mainly two sources of attack, i.e., the vehicle and the RSU. Attacks that can be launched by the vehicle are similar to V2VC attacks and have been extensively explored [9]–[11]. In this section, we mainly focus on detection mechanisms for attacks launched by a compromised RSU. To defend the network from attacks like man in the middle and eavesdropping, authors in [12] presented a protocol for mutual authentication between the provider and the consumer. Rogue mobile edges can be

Manuscript received September 3, 2021 revised May 24, 2022; approved for publication by Jeongyeup Paek Division 3 Editor, June 29, 2022.

N. V. Abhishek is with the Information and Communication Technology Cluster, Singapore Institute of Technology, email: nvenkataabhishek@gmail.com.

T. J. Lim is with the School of Electrical and Information Engineering, University of Sydney, email: tj.lim@sydney.edu.au.

T. J. Lim is the corresponding author.

Digital Object Identifier: 10.23919/JCN.2022.000026

1229-2370/22/$10.00 © 2022 KICS

detected using the detection systems provided in [13]. The round trip time of a packet exchanged between the user and the DNS server is used to detect the rogue nodes. In [14], the authors proposed Wi-Fi malicious rogue access point finder (RAF) to detect the presence of rogue nodes. RAF can be installed on any device without any special requirement. RAF detects the existence of a malicious rogue access point (AP) based on different reverse traceroute information, i.e., the set of IPs of the devices traversed by the packet. A remote server collects this information. The authors presume that the packet's route will be different, but the adversary may likely match the path of the packet.

Authors in [15] present a mechanism to detect the presence of powerful hardware-based rogue access points (PrAPs). The detection algorithm uses a dedicated device called PrAP-Hunter and is based on intentional channel interference. The detection algorithm requires additional devices to be deployed and may be a viable option for large networks. To address the issue of a rogue node, a discrete event system (DES) based detection system is proposed in [16]. The detector proposed is a state estimator that keeps track of the system using events and alerts if the system moves into an attack state. In [17], the authors proposed an evil twin detection and mitigation framework called "EvilScout". The framework utilizes the information of the IP prefix distribution by the Legitimate AP. However, the performance of the above two detection systems is limited by the data available. Another major attack that could disrupt the communication between the vehicles and the edge servers is jamming the wireless channel. The authors in [18] introduce two algorithms for countering stochastic jamming and adversarial jamming. Malicious cloudlets present in LTE networks can be detected using the reputation-based trust management system presented in [19]. The system limits the effect of dishonest ratings and prevents cloudlets from modifying the ratings from mobile users.

In our previous work in [20], [21], we considered only an adversarial RSU that corrupts packets to be forwarded to the vehicles (i.e., downlink packets are maliciously dropped). We proposed a trust-based intrusion detection system (IDS) to detect the adversary. With trust values obtained using the estimated attack probability that was obtained using maximum likelihood estimation (MLE). Since we could not get closed-form expressions for the estimate, we used the weighted least square approach to obtain the same in this paper. Using the Neyman-Fischer factorization theorem, we also prove that the statistics used for obtaining the downlink trust value are sufficient. Also, bounds on the mean and variance of the estimated downlink attack probability are presented. This paper additionally presents a detection system to identify an adversarial RSU that drops uplink packets. With this feature, our method defends against an attacker using the RSU to attack only the uplink or the downlink or both.

B. Our Contribution

In this paper, we consider that the adversary has obtained root access to an RSU and is disrupting the communication between the RSU and the vehicles. The adversary considered in this paper mimics a bad radio channel between the vehicles and the RSU. Therefore, the adversary can successfully increase the computation and communication latencies by launching such an attack and creating a substantial additional delay in the network. This mainly affects delay-sensitive applications and also leads to wastage of edge computing resources. In this paper, we introduce a trust-based IDS for such attacks. The key novelty behind the IDSs proposed in this paper is the use of the measured packet drop rate (on the downlink) and packet retransmission rate (on the uplink) between vehicles and RSUs. The downlink IDS relies on vehicles recording the wireless channel quality in terms of packet drop rate. The uplink IDS relies on vehicles recording the packet retransmission rate. We also present a mechanism to detect the presence of any malicious vehicles trying to deceive the detection systems into falsely classifying an RSU. For example, vehicles can report low trust values about benign RSUs and make the detection system classify the benign RSU as malicious.

C. Organization

The rest of the paper is organized as follows. In Section II, the network and the adversary models are described. Section III presents the downlink detection system and obtains sufficient statistics and bounds on the mean and variance of the downlink attack probability. We also present a mechanism to detect malicious vehicles that are trying to deceive the IDS. In Section IV, we present the uplink detection system and a mechanism to detect malicious vehicles. In Section V, results are presented to demonstrate the performance of the proposed detection algorithms. Finally, in Section VI, we conclude our paper and provide some directions for future work.

II. System Model

A. Network Model

A vehicular network with the hierarchical architecture indicated in Fig. 1 is considered. The vehicles in the network are denoted using $V_j, j \in \{1, 2, \cdots\}$. The roadside units (RSUs) are denoted using $R_i, i \in \{1, 2, \cdots\}$. The RSUs are further connected to RSU gateways (RSUGs). Each RSU is connected to only one RSUG. Also, at a given instant, a vehicle V_j is connected to only one RSU. When the vehicle moves away from a previously connected RSU, say R_i, it connects to a new RSU, say R_k, which provides better signal to noise ratio (SNR) than R_i. Each RSU is equipped with a Mobile Edge host that enables MEC. Such a model is proposed in both IEEE 802.11 and 5G cellular networks [3]. There will be a non-zero probability of decoding a packet in error for any given network in normal operation due to various network imperfections. Packet errors occur on both the uplink and downlink. We assume a retransmission protocol is used in both links, i.e., every dropped packet is retransmitted until successfully received, or the communication is timed out.

A corrupted packet can be detected at the receiver using the cyclic redundancy check (CRC) code embedded in the MAC

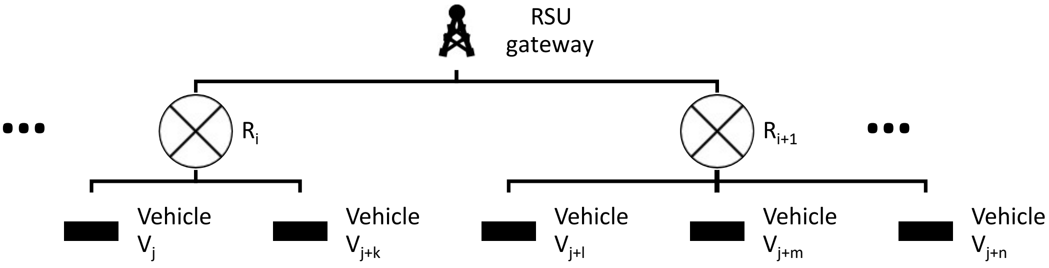

Fig. 1. Network model illustration.

layer payload. Due to mobility, the natural PDP[1] of packets transmitted between the same RSU-vehicle pair at different times may differ significantly. The proposed algorithm requires the natural PDP to be known or estimated. To estimate the packet drop probability of every downlink packet received by the vehicle, we can assume that a vehicle has access to a signal quality indicator. There are three quantities that can be measured at a receiver which strongly correlates with PDP: Signal to noise ratio, link quality indicator (LQI), and received signal strength indicator (RSSI). RSSI provides the signal strength of the received packet. When there are no transmissions, the RSSI is equal to the noise floor. SNR is typically given by the difference in decibel between the pure (i.e., without noise) received signal strength and the noise floor. LQI is measured based on the first eight symbols of the received packet as a score ranging from 50 to 110 (higher values are better). These three measures are related, but SNR is known to be the best indicator for characterizing the quality of the link [22]. In this paper, the SNR will be used by the vehicles to obtain the PDP of the downlink packets. For the uplink packets, such signal quality indicators cannot be assumed to be known by the vehicle.

B. Adversary Model

We assume that the adversary that has compromised one or more RSUs disrupts the communication between vehicles and the RSUs. The adversary can launch many attacks that impact message security, quality of service, etc., using the compromised RSU. Attacks that compromise message security by eavesdropping, stealing credentials, etc., can be taken care of using cryptography. Attacks that focus on service interruption, e.g., jamming, black hole, selective forwarding, etc., have been thoroughly explored and can be countered using already proposed detection systems in the literature [12], [13], [18], [19]. These attacks can be detected with high reliability and therefore are not addressed in this paper. The adversary considered in this paper implements the following strategies:

1) On the downlink, the compromised RSU, say R_i, selectively modifies a packet to be transmitted to the vehicle V_j with a probability that is unknown and denoted by δ_{ij}^d. The adversary can achieve this by flipping some of the bits of the physical layer payload and/or corrupting the channel pilots used for channel estimation and equalization. When the vehicle receives such a packet, it will be dropped because the CRC check failed, and a request for re-transmission will be sent.
2) On the uplink, the compromised RSU, say R_i, selectively drops a packet received from a vehicle V_j with a probability that is unknown and denoted by δ_{ij}^u. Then, the adversary deliberately makes the vehicle re-transmit the dropped packet by sending a negative acknowledgment.

The increased packet transmission delay disrupts time-sensitive services, leading to possibly severe safety consequences. Also, this increases the number of simultaneous transmissions, increasing the number of packet collisions and resulting in an effective radio range reduction. Applications where delay and network availability are significant factors like road safety, traffic efficiency, etc., can get severely affected. Such attacks are difficult to detect because they mimic a poor radio channel.

C. Packet Drop Probabilities

Firstly, we calculate the PDP of the downlink packets in the presence of attack given the PDP in the absence of attack. For every kth packet $k \in \{1, 2, \cdots\}$, sent by R_i and received by vehicle V_j, the PDP of the kth packet is estimated as follows:

1) Firstly the SNR of the packet is estimated and the corresponding symbol error rate $s_{ij,k}^d$ is obtained using standard models [23].
2) The packet is dropped when at least one symbol is received in error. Therefore the PDP, using the obtained symbol error rate, is estimated as:

$$\alpha_{ij,k}^d = 1 - \ (1 - s_{ij,k}^d)^m, \tag{1}$$

where m is the number of symbols present in a packet.

In the event of an attack, a packet drop is either due to poor channel conditions or due to the RSU's misbehavior. When the RSU misbehaves, a packet drop occurs for sure. When the RSU chooses not to corrupt the packet, the packet drop occurs due to the poor channel conditions. More precisely, in the presence of attack, the PDP of the kth packet increases to

$$\beta_{ij,k}^d = \delta_{ij}^d + \ (1 - \delta_{ij}^d)\alpha_{ij,k}^d, \tag{2}$$

where δ_{ij}^d is the attack probability on each packet. In the absence of the attack, $\beta_{ij,k}^d = \alpha_{ij,k}^d$ i.e., δ_{ij}^d is equal to zero. For the uplink case, the PDP in the absence of the attack

[1] Packet drop probability in the absence of attack.

cannot be estimated by the vehicle since the SNR of the packet received by the RSU is not accessible to the vehicle. However the relation between the PDPs in the presence and absence of attack is similar to (2) i.e.,

$$\beta^u_{ij,k} = \delta^u_{ij} + \; (1-\delta^u_{ij})\alpha^u_{ij,k}, \tag{3}$$

where $\beta^u_{ij,k}$ is the PDP of the kth packet in the presence of attack, $\alpha^u_{ij,k}$ is the PDP of the kth packet in the absence of attack and δ^u_{ij} is the attack probability. Similar to the downlink case, in the absence of the attack, $\beta^u_{ij,k} = \alpha^u_{ij,k}$ i.e., δ^u_{ij} is equal to zero.

D. Intrusion Detection System

We propose to implement trust-based Intrusion Detection Systems for detecting adversaries executing the attacks in Section II-B. Trust-based detection systems that have been proposed in the recent literature are attractive methods to deal with security threats in highly distributed and dynamic scenarios. This methodology is adopted in the VNET scenario precisely for this reason. The detection algorithm is divided into three phases that are listed below:

1) **Trust calculation:** The individual vehicle's trust level towards the RSU will be calculated at the vehicle's end. The trust value, for downlink packets, calculated by vehicle V_j for RSU R_i is denoted by Θ^d_{ij}. For the case of uplink packets, the trust value is represented by Θ^u_{ij}. These trust values will be relayed to the RSU Gateway via an RSU other than R_i.
2) **Trust aggregation:** At regular intervals, the trust values obtained from all the vehicles towards a given RSU will be combined (at the RSU Gateway) to get an aggregated trust value for that RSU. The aggregated trust value, for downlink, for R_i is denoted by Θ^d_i and for uplink is represented by Θ^u_i.
3) **Adversary detection:** Once the aggregated trusts are available, they are compared against thresholds, Γ_u for uplink and Γ_d for downlink, to detect the adversary's presence.

In this paper, we also consider that a small percentage of vehicles can be malicious. Malicious vehicles are those that try to trick the detecting system into labeling a benign RSU as malicious or vice versa. Using the aggregated and individual trust values of different RSUs, we estimate a similarity metric that will be used to identify the presence of malicious vehicles.

III. Downlink Intrusion Detection System

In this section, we present the detection system for attacks on downlink packets. The detection algorithm, for RSU R_i, based on the feedback from a set of vehicles $\mathcal{V}_i$, is presented.

A. Individual Trust Evaluation

TABLE I
List of symbols used in the paper.

Symbol	Description
$\alpha^d_{ij,k}$	PDP of the kth downlink packet in the absence of attack
$\beta^d_{ij,k}$	PDP of the kth downlink packet in the presence of attack
$\alpha^u_{ij,k}$	PDP of the kth uplink packet in the absence of attack
$\beta^u_{ij,k}$	PDP of the kth uplink packet in the presence of attack
δ^d_{ij}	Downlink attack probability of R_i for V_j
δ^u_{ij}	Uplink attack probability of R_i for V_j
Θ^d_{ij}	V_j's individual downlink trust value for R_i
Θ^u_{ij}	V_j's individual uplink trust value for R_i
Θ^d_i	Aggregated downlink trust value of R_i
Θ^u_i	Aggregated uplink trust value of R_i
Γ_d	Threshold for downlink IDS
Γ_u	Threshold for uplink IDS
$B^d_{ij,k}$	Denotes whether kth downlink packet is dropped ot not
$B^u_{ij,k}$	Denotes whether kth uplink packet is dropped ot not
w^d_{ij}	Weight of V_j's individual downlink trust value
w^u_{ij}	Weight of V_j's individual uplink trust value
$\hat{\delta}^d_{ij}$	Estimated value of δ^d_{ij}
μ^d_{ij}	Mean of $\hat{\delta}^d_{ij}$
σ^d_{ij}	Standard Deviation of $\hat{\delta}^d_{ij}$
p_{ij}	Uplink packet retransmission rate of V_j
ρ^d_j	Downlink similarity measure of V_j
γ^d_j	Downlink threshold to detect malicious vehicles
ρ^u_j	Uplink similarity measure of V_j
γ^u_j	Uplink threshold to detect malicious vehicles
N^d_{ij}	Number of packets transmitted on the link $R_i \rightarrow V_j$
N^u_{ij}	Number of packets transmitted on the link $V_j \rightarrow R_i$

In this section, we compute Θ^d_{ij}, vehicle V_j's individual trust value for RSU R_i. Unfortunately trust as a concept has no universally accepted definition. The trust value must somehow dynamically reflect the behavior of the RSU. Therefore, we adopt the following definition of trust based on the attack probability δ^d_{ij}. Since this is an unknown parameter, we need to obtain the estimated value, denoted by $\hat{\delta}^d_{ij}$, using the following proposed method:

1) We first introduce the variable $B^d_{ij,k}$, defined as follows. If the kth packet, transmitted by R_i, is received successfully by V_j, then $B^d_{ij,k} = 0$, otherwise $B^d_{ij,k} = 1$. Given that there are only two outcomes, we can assume that $B^d_{ij,k}$ follows Bernoulli distribution and define the probability mass function (PMF) of $B^d_{ij,k}$ as follows:
$$P(B^d_{ij,k} = b; \delta^d_{ij}) = \; (\beta^d_{ij,k})^b \; (1-\beta^d_{ij,k})^{(1-b)}, \tag{4}$$
for $b \in \{0,1\}$, where $\beta^d_{ij,k}$ was defined in (2). The expected value of $B^d_{ij,k}$, for a given δ^d_{ij}, is $\beta^d_{ij,k}$.
2) Using the weighted least squares approach [24], we obtain an estimate of δ^d_{ij} by minimizing
$$J(\delta^d_{ij}) = \sum_{k=1}^{N^d_{ij}} w^d_{ij,k} \; (B^d_{ij,k} - \beta^d_{ij,k})^2, \tag{5}$$
where $w^d_{ij,k}$ are the weights and N^d_{ij} is the total number of packets transmitted by R_i to V_j. The weights are

chosen such that the contributions of reliable samples[2] are emphasized. The weight $w^d_{ij,k}$ is defined as

$$w^d_{ij,k} = \frac{1}{(\alpha^d_{ij,k})(1-\alpha^d_{ij,k})}, \forall k. \tag{6}$$

By equating the first derivative of (5) with respect to δ_{ij} to zero, we obtain

$$\hat{\delta}^d_{ij} = \max\ (0, \delta'_{ij}), \tag{7}$$

where

$$\delta'_{ij} = \frac{\sum_{k=1}^{N^d_{ij}}\left(\frac{B^d_{ij,k}}{\alpha^d_{ij,k}}-1\right)}{\sum_{k=1}^{N^d_{ij}}\left(\frac{1}{\alpha^d_{ij,k}}-1\right)}. \tag{8}$$

3) Using the obtained $\hat{\delta}^d_{ij}$, we now define

$$\Theta^d_{ij} = 1-\hat{\delta}^d_{ij}. \tag{9}$$

B. Estimated Attack Probability: Mean and Variance

Given the expression in (7), estimating the mean μ^d_{ij} and variance $(\sigma^d_{ij})^2$ of $\hat{\delta}^d_{ij}$ is difficult. In this section we calculate bounds on both the mean and variance, for a given δ^d_{ij}. From (7), the following can be established.

$$\delta'_{ij} \le \hat{\delta}^d_{ij} \quad \Rightarrow \quad E[\delta'_{ij}] \le E[\hat{\delta}^d_{ij}] \tag{10}$$

$${\delta'_{ij}}^2 \ \ge \ (\hat{\delta}^d_{ij})^2 \quad \Rightarrow \quad E[{\delta'_{ij}}^2] \ge E[(\hat{\delta}^d_{ij})^2] \tag{11}$$

$E[x]$ refers to the expected value of the random variable x. Using these, the following can be inferred:

$$E[(\hat{\delta}^d_{ij})^2] - \ (E[\hat{\delta}^d_{ij}])^2 \le E[{\delta'_{ij}}^2] - \ (E[\delta'_{ij}])^2. \tag{12}$$

The variable δ'_{ij} is a weighted sum of independent Bernoulli variables. Therefore, the expectation of δ'_{ij} is the weighted sum of the mean of each Bernoulli variable i.e.,

$$\begin{aligned} E[\delta'_{ij}] &= \frac{1}{\sum_{k=1}^{N^d_{ij}}\left(\frac{1}{\alpha^d_{ij,k}}-1\right)} \sum_{k=1}^{N^d_{ij}}\left(\frac{E[B^d_{ij,k}]}{\alpha^d_{ij,k}}-1\right) \\ &= \frac{1}{\sum_{k=1}^{N^d_{ij}}\left(\frac{1}{\alpha^d_{ij,k}}-1\right)} \sum_{k=1}^{N^d_{ij}}\left(\frac{\beta^d_{ij,k}}{\alpha^d_{ij,k}}-1\right). \end{aligned} \tag{13}$$

The variance of δ'_{ij} is calculated as:

$$\begin{aligned} V[\delta'_{ij}] &= \left(\frac{1}{\sum_{k=1}^{N^d_{ij}}\left(\frac{1}{\alpha^d_{ij,k}}-1\right)}\right)^2 \sum_{k=1}^{N^d_{ij}} \frac{V[B^d_{ij,k}]}{(\alpha^d_{ij,k})^2} \\ &= \left(\frac{1}{\sum_{k=1}^{N^d_{ij}}\left(\frac{1}{\alpha^d_{ij,k}}-1\right)}\right)^2 \sum_{k=1}^{N^d_{ij}} \frac{(\beta^d_{ij,k})(1-\beta^d_{ij,k})}{(\alpha^d_{ij,k})^2}, \end{aligned} \tag{14}$$

where $V[x]$ denotes the variance of the random variable x. Using (13) and (14), the lower bound on the mean and the upper bound on the variance of $\hat{\delta}^d_{ij}$ can be derived as

$$\mu^d_{ij} \ \ge \ \delta^d_{ij}, \tag{15}$$

$$\begin{aligned} (\sigma^d_{ij})^2 \ \le \ & \frac{(\delta^d_{ij})(1-\delta^d_{ij})}{\left(\sum_{k=1}^{N^d_{ij}}\left(\frac{1}{\alpha^d_{ij,k}}-1\right)\right)^2} \sum_{k=1}^{N^d_{ij}}\left(\frac{1}{\alpha^d_{ij,k}}-1\right)^2 \\ & + \frac{1-\delta^d_{ij}}{\sum_{k=1}^{N^d_{ij}}\left(\frac{1}{\alpha^d_{ij,k}}-1\right)}. \end{aligned} \tag{16}$$

The variance decreases as we increase the attack probability. Therefore, for a higher δ^d_{ij}, a more accurate estimate can be expected.

C. Sufficient Statistics

We now obtain the sufficient statistics required for estimating the attack probability δ^d_{ij}. For this, we need the joint distribution of the variables $B^d_{ij,k}, k \in \{1,2,\cdots,N^d_{ij}\}$. The packet transmissions between R_i and V_j occur over a highly mobile wireless channel. Therefore, we can assume that the packet drop events for two separate packets are independent. Hence, the joint probability distribution of the variables $B^d_{ij,k}, k \in \{1,2,\cdots,N^d_{ij}\}$ is given by the product of their individual probability distributions, as shown below.

$$P(B^d_{ij} = b^d_{ij}; \delta^d_{ij}) = \prod_{k=1}^{N^d_{ij}} \ (\beta^d_{ij,k})^{b^d_{ij,k}} \ (1-\beta^d_{ij,k})^{(1-b^d_{ij,k})}, \tag{17}$$

where $B^d_{ij} = \{B^d_{ij,1}, B^d_{ij,2}, \cdots, B^d_{ij,N^d_{ij}}\}$, $b^d_{ij} = \{b^d_{ij,1}, b^d_{ij,2}, \cdots, b^d_{ij,N^d_{ij}}\}$ and N^d_{ij} is the total number of packets received by the vehicle V_j from RSU R_i. Note that the joint PDF can be factorized as

$$\begin{aligned} P(B^d_{ij} = b^d_{ij}; \delta^d_{ij}) =& g(T_1(b^d_{ij}), T_2(b^d_{ij}), \cdots, T_{N^d_{ij}}(b^d_{ij})) \\ & \times h(b^d_{ij}), \end{aligned} \tag{18}$$

where the functions $G \triangleq g(T_1(b^d_{ij}), \cdots, T_{N^d_{ij}}(b^d_{ij}))$, $T_1(b^d_{ij}), \cdots, T_{N^d_{ij}}(b^d_{ij})$ and $h(b^d_{ij})$ are defined below.

$$G \ = \ \prod_{k=1}^{N^d_{ij}} (1-\beta^d_{ij,k}) \left(\frac{\beta^d_{ij,k}}{1-\beta^d_{ij,k}}\right)^{T_k(b^d_{ij})} \tag{19}$$

$$T_k(b^d_{ij}) \ = \ b^d_{ij,k}, \forall k \tag{20}$$

$$h(b^d_{ij}) \ = \ 1 \tag{21}$$

Therefore, using the Neyman-Fischer factorization theorem, $b^d_{ij,k}, k \in \{1, \cdots, N_{ij}\}$ are jointly sufficient statistics for the attack probability δ^d_{ij} and hence sufficient for the trust value Θ^d_{ij}. Our estimate of δ^d_{ij} in (8) is thus based on jointly sufficient statistics.

[2] Defined as those channels with small variance of $B^d_{ij,k}$.

D. Trust Aggregation and Detection Algorithm

We refer to aggregation as a process of combining the trust values reported by different vehicles. Aggregating these trust values reduces the uncertainty of the detection system. maximum, minimum, average, and weighted sum are the most widely used aggregation operators [25]. Due to the estimation errors in computing $\hat{\delta}^d_{ij}$, the trust values computed by vehicles for a malicious RSU can be high even in the presence of an attack. Therefore, if the maximum aggregation operator is used, the detection system would result in classifying a malicious RSU as benign with a non-negligible probability. Similarly, in the absence of an attack, due to the erroneously obtained $\hat{\delta}^d_{ij}$, the trust values computed for a benign RSU can be smaller. Therefore, if the minimum aggregation operator is used, the detection system would result in classifying a benign RSU as malicious with a non-negligible probability. The reliability of each vehicle's computed trust value depends on the number of packets they observe. As different vehicles may receive different numbers of packets average aggregation will not be appropriate. Therefore a weighted sum, with weights based on the number of packets received, is proposed to obtain the aggregated trust value. Using the individual trust values reported by the vehicles $V_j, j \in \mathcal{V}_i$, the aggregated trust value Θ^d_i is defined as

$$\Theta^d_i = \sum_{j\in\mathcal{V}_i} \omega^d_{ij}\Theta^d_{ij}, \tag{22}$$

where ω^d_{ij} is the weight given to the trust value computed by vehicle $V_j, j \in \mathcal{V}_i$. The accuracy of estimated attack probability increases with the number of packets N^d_{ij}. Therefore the weights are assigned in proportion to the number of packets N^d_{ij}, i.e., the number of packets transmitted from R_i to V_j.

$$\omega^d_{ij} = \frac{N^d_{ij}}{\sum_{j\in\mathcal{V}_i} N^d_{ij}} \tag{23}$$

With the aggregated trust available, the detection system decides that RSU R_i is malicious on the downlink if

$$\Theta^d_i \leq \Gamma_d. \tag{24}$$

The expression for the aggregated trust is

$$\Theta^d_i = \sum_{j\in\mathcal{V}_i} \omega^d_{ij}\left(1 - \max\left(0, \frac{\sum_{k=1}^{N^d_{ij}} \frac{B^d_{ij,k}}{\alpha^d_{ij,k}} - N^d_{ij}}{\sum_{k=1}^{N^d_{ij}} \frac{1}{\alpha^d_{ij,k}} - N^d_{ij}}\right)\right). \tag{25}$$

It can be seen that obtaining the distribution of Θ^d_i is not trivial. Exact analytical expressions for the performance characteristics, i.e., false alarm and missed detection probabilities, are therefore unavailable. So, we propose to obtain the threshold value heuristically. Let us say that the estimate of attack probabilities, i.e., $\{\hat{\delta}_{ij}, j \in \mathcal{V}_i\}$, in the absence of attack is mostly less than ϵ_d. Hence, the minimum accepted individual trust values computed from (9) will be equal to $(1-\epsilon_d)$. This implies that the accepted aggregated trust will be $(1-\epsilon_d)$, and hence we assign it as the threshold value.

IV. Uplink Intrusion Detection System

In this section, we present the detection system for attacks on uplink traffic. The detection algorithm, for RSU R_i, based on the feedback from a set of vehicles $\mathcal{V}_i$, is presented. Unlike downlink packets, we cannot assume that the uplink packets' packet retransmission rate (PRR) will be accessible to the vehicles. Hence the detection system proposed in (24) cannot be modified like in [20] to identify the malicious RSU. Therefore, we first find sufficient statistics for estimating the attack probability δ^u_{ij} and use them for obtaining the trust value using fuzzy logic.

A. Sufficient Statistics

We first introduce the variable $B^u_{ij,k}$, defined as follows. If the kth packet, transmitted by RSU R_i, is received successfully by V_j, then $B^u_{ij,k} = 0$, otherwise $B^u_{ij,k} = 1$. The probability distribution function (PDF) of $B^u_{ij,k}$ is

$$P(B^u_{ij,k} = b; \delta^u_{ij}) = (\beta^u_{ij,k})^b \, (1-\beta^u_{ij,k})^{(1-b)}, \tag{26}$$

for $b \in \{0,1\}$. The joint probability distribution of the variables $B^u_{ij,k}, k \in \{1,2,\cdots,N^u_{ij}\}$. Since the packet transmissions between R_i and V_j occur over a highly mobile wireless channel, we can assume that the event of the k_1th packet ($k_1 \in \{1,2,\cdots,N^u_{ij}\}$) being dropped is independent of k_2th packet ($k_2 \in \{1,\cdots,k_1-1,k_1+1,\cdots,N^u_{ij}\}$) being dropped. Hence, the joint probability distribution of the variables $B^u_{ij,k}, k \in \{1,2,\cdots,N^u_{ij}\}$ is given by the product of their individual probability distributions, as shown below:

$$P(B^u_{ij} = b^u_{ij}; \delta^u_{ij}) = \prod_{k=1}^{N^u_{ij}} (\beta^u_{ij,k})^{b^u_{ij,k}} \, (1-\beta^u_{ij,k})^{(1-b^u_{ij,k})}, \tag{27}$$

where $B^u_{ij} = \{B^u_{ij,1}, B^u_{ij,2}, \cdots, B^u_{ij,N^u_{ij}}\}$, $b^u_{ij} = \{b^u_{ij,1}, b^u_{ij,2}, \cdots, b^u_{ij,N^u_{ij}}\}$ and N^u_{ij} is the total number of packets received by the vehicle V_j from RSU R_i. The joint PDF, similar to the downlink case, can be factorized as

$$\begin{aligned} P(B^u_{ij} = b^u_{ij}; \delta^d_{ij}) =& g(T_1(b^u_{ij}), T_2(b^u_{ij}), \cdots, T_{N^u_{ij}}(b^u_{ij})) \\ & \times h(b^u_{ij}), \end{aligned} \tag{28}$$

where the functions $G \triangleq g(T_1(b^u_{ij}), \cdots, T_{N^u_{ij}}(b^u_{ij}))$, $T_1(b^u_{ij}), \cdots, T_{N^u_{ij}}(b^u_{ij})$ and $h(b^u_{ij})$ are defined as

$$G = \prod_{k=1}^{N^u_{ij}} (1-\beta^u_{ij,k}) \left(\frac{\beta^u_{ij,k}}{1-\beta^u_{ij,k}}\right)^{T_k(b^u_{ij})}, \tag{29}$$

$$T_k(b^u_{ij}) = b^u_{ij,k}, \forall k, \tag{30}$$

$$h(b^u_{ij}) = 1. \tag{31}$$

Therefore, using Neyman-Fischer factorization theorem, the statistics $T_1(b^u_{ij}), T_2(b^u_{ij}), \cdots, T_{N^u_{ij}}(b^u_{ij})$ are jointly sufficient statistics for the attack probability δ^u_{ij} and hence sufficient for constructing the trust value Θ^u_{ij}.

B. Individual Trust Evaluation

We compute the vehicle V_j's individual trust value i.e., Θ^u_{ij} for RSU R_i. We propose to obtain the trust values using fuzzy logic based on the following rules:

1) For low values of packet retransmission rate, we can assume that the probability of an attack being implemented is low and therefore assign high trust values. Specifically, if the packet retransmission rate is equal to zero, the trust value equals one.
2) We can suppose that the possibility of an attack being carried out is high when the packet retransmission rate is high and hence assign low trust levels. Specifically, if the packet retransmission rate is equal to one, the trust value equals zero.
3) When the packet retransmission rate is moderate, the uncertainty in determining the presence of an attack is high. Therefore, we assign average trust values.

We follow the below procedure to obtain the trust values.

1) We use the variables $B^u_{ij,k}, k \in \{1, 2, \cdots, N^u_{ij}\}$ to calculate the average packet retransmission rate, denoted by p_{ij}. The PRR is calculated as the ratio of packets retransmitted to the total number of packets transmitted. The PRR is calculated as follows:

$$p_{ij} = \frac{\sum_{j=1}^{N^u_{ij}} B^u_{ij,k}}{N^u_{ij}}, \tag{32}$$

where N^u_{ij} is the number of packets forwarded by V_j.

2) We use the sigmoid function [26] to generate the trust values. Using the obtained p_{ij}, we now define

$$\Theta^u_{ij} = \frac{1 + \exp(2)}{1 + \exp(\frac{2}{1-p_{ij}})}. \tag{33}$$

It can be seen that the expression for the trust satisfies the rules stated previously.

C. Trust Aggregation and Detection Algorithm

Similar to the aggregation mechanism followed in (22), we use weighted sum to obtain the aggregated trust value Θ^u_i which is defined as

$$\Theta^u_i = \sum_{j \in \mathcal{V}_i} \omega^u_{ij} \Theta^u_{ij}, \tag{34}$$

where ω^u_{ij} is the weight of the vehicle $V_j, j \in \mathcal{V}_i$ and $\Theta^u_{ij}, j \in \mathcal{V}_i$ are the individual trust values reported by the vehicles. The accuracy of the PRR of vehicle V_j increases with an increasing number of packets N^u_{ij} implying that the uplink trust value can be estimated with better accuracy. As a result, the weights are proportional to the number of packets N^u_{ij}, i.e., the number of packets sent from V_j to R_i.

$$\omega^u_{ij} = \frac{N^u_{ij}}{\sum_{j=1}^{M} N^u_{ij}} \tag{35}$$

Using the aggregated trust in (34), the detection system decides the presence of the attack if

$$\Theta^u_i = \sum_{j \in \mathcal{V}_i} \omega^u_{ij} \left(\frac{1 + \exp(2)}{1 + \exp(\frac{-2}{p_{ij}-1})} \right) \leq \Gamma^u_i. \tag{36}$$

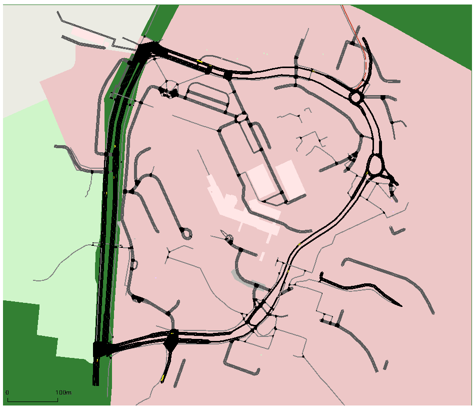

Fig. 2. Real-life traffic scenario.

Obtaining the expressions for false alarm and missed detection probabilities is difficult since they would depend on many unknown variables (i.e., $\{\alpha^u_{ij,k}, \forall k, j \in \mathcal{V}_i\}$ and $\{\delta^u_{ij}, j \in \mathcal{V}_i\}$). We therefore heuristically obtain the threshold value. In the absence of attack, the acceptable maximum PRRs i.e., $\{p_{ij}, j \in \mathcal{V}_i\}$ is equal to ϵ_u. Hence, the minimum individual trust values computed from (33) will be equal to $\exp\left(-2\epsilon_u/(1-\epsilon_u)\right)$. This implies that the minimum aggregated trust will be $\exp\left(-2\epsilon_u/(1-\epsilon_u)\right)$ and hence we assign it as the threshold value.

V. RSU Detection Delay

Let's say the proposed algorithm evaluates the network for every M_F number of vehicles leave the network. Since each vehicle transmits one feedback packet, the total number of feedback packets are also equal to M_F. Therefore, there will be a delay in identifying the compromised RSU. To analyze the same, we used urban mobility (SUMO) simulation package with OSMWebWizard. Consider a part of the region of the National University of Singapore, shown in Fig. 2 with vehicles and buses moving with no pause. The vehicle density can be increased by increasing the value of the parameter "Number of vehicles per km per hour" available in the SUMO simulator. The average time taken by the algorithm to detect a compromised RSU for different vehicular densities for the network in Fig. 2 is presented in Fig. 3. It can be seen that the time taken to detect a malicious RSU is high when the vehicle density is high. Also, a higher number of vehicles in decision-making improves the accuracy of the detection algorithm. However, it takes more time to make the decision.

VI. Malicious Vehicle Identification

In this section, the detection mechanism for identifying the malicious vehicles reporting false feedback is explained in detail. The objective of these vehicles is to deceive the detection system into classifying a benign RSU as malicious or vice versa. For example, let us say a malicious vehicle V_j is trying to influence the IDS into classifying a benign RSU R_i as malicious. To make it appear as if the attack probability of

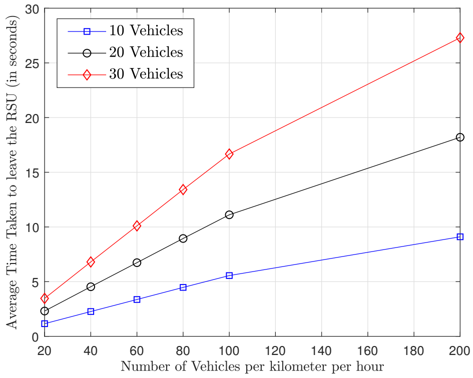

Fig. 3. Average time taken for the detection algorithm to identify the corrupt RSU.

R_i equal to $\delta_v > 0$, the vehicle V_j generates the trust values as follows:

1) **Downlink trust value:** When the kth packet is received by the vehicle, irrespective of whether it is in error or not, the value of $B^d_{ij,k}$ is decided using a Bernoulli distribution with probability δ_v. Therefore, the packet drop rate observed would be equal to δ_v, and the trust according to 9 will be equal to $1 - \delta_v$.
2) **Uplink trust value:** When the kth packet is transmitted, irrespective of whether it is received by the RSU or not, the value of $B^u_{ij,k}$ is decided using a Bernoulli distribution with probability δ_v. Therefore, the packet retransmission rate observed would be equal to δ_v and the trust according to (33) will be equal to $\frac{1+\exp(2)}{1+\exp(\frac{2}{1-\delta_v})}$.

If the vehicle wants to influence the IDS into classifying a malicious RSU as benign, then the vehicle relays very high trust values despite the RSU's behavior. Such vehicles need to be identified since they can have a significant impact on the IDS. Firstly, we focus on the vehicles affecting the downlink detection algorithm. The key observation used is that there will be a huge gap between trust values reported by the malicious vehicles and the trust values of the RSUs. This implies that the distance between $L^d = \{\Theta^d_1, \cdots, \Theta^d_K\}$ and $L^d_j = \{\Theta^d_{1j}, \cdots, \Theta^d_{Kj}\}$ will be large if V_j is giving false feedback. We, therefore, need a metric that can calculate the similarity between L^d_j and L^d. One possible metric is the Gaussian kernel similarity measure [27]. For V_j, it is calculated as:

$$\rho^d_j = \exp(-\left\|L^d - L^d_j\right\|^2). \tag{37}$$

The value of ρ^d_j computed in (37) is now compared to a preset threshold γ^d_j to decide whether V_j is malicious or not, i.e., we decide that the (downlink) trust is false if and only if

$$\rho^d_j \leq \gamma^d_j. \tag{38}$$

The detection for the uplink case is similar to the downlink, i.e., we decide the (uplink) feedback is false if and only if

$$\rho^u_j \leq \gamma^u_j, \tag{39}$$

where $\rho^u_j = \exp(-\left\|L^u - L^u_j\right\|^2)$, $L^u = \{\Theta^u_1, \cdots, \Theta^u_K\}$ and $L^u_j = \{\Theta^u_{1j}, \cdots, \Theta^u_{Kj}\}$.

VII. Simulation Results

We present results to demonstrate the following in this section. The results were generated using MATLAB. The results were generated using the vehicle model illustrated in Fig. 4. The length of the road considered is 300 meters, and the RSU R_1 is placed at its midpoint. The road is divided into 600 slots, and therefore the distance between the RSU and a vehicle present in the Uth slot is given by $|U - 300|/2$. In every time slot, the vehicle moves one slot. For every 30 time slots, a new vehicle arrives into the 1st slot and connects to R_1. Once a vehicle moves out of the 600th slot, it loses its connection with R_1. Hence, at any time, there are 20 vehicles on the road. In every time slot, using a uniform distribution in MATLAB, we decide which vehicle is transmitting. At the maximum, only one packet is transmitted in a single time slot. The path loss model in [28] is used where $L_0 = -47$ dB and $x = -3$. The transmit power is 20 dBm and the noise variance (additive) is -100 dBm. The PDP is calculated using the symbol rate expressions in [23]. The expressions for 16 QAM transmission in Rayleigh fading channels are used for the same.

A. Downlink IDS - Estimated Attack Probability

To demonstrate that the mean of the least square estimate, of vehicle V_6, is close to its actual value, i.e., $\hat{\delta}^d_{16}$ is close to δ^d_{16}, we ran the following steps:

1) For a given value of $\delta^d_{16} \triangleq \delta$, we determine the number of packets dropped for the vehicle V_6.
2) We then calculate the value of $\hat{\delta}^d_{16}$ using (7).
3) The simulated values obtained over 10^5 Monte Carlo simulations are averaged for each value of δ. The obtained averages are shown in Fig. 5. The average value is denoted using $\hat{\delta}$.

It can be seen from Fig. 5 that the average estimated value is almost equal to the actual value in all the cases.

B. Performance Characteristics

The performance of IDSs are generally characterized using false alarm and missed detection probabilities. The probability that the detection system decides that a malicious RSU is authentic is referred to as missed detection probability, and the probability that a benign RSU is classified as malicious is called false alarm probability i.e.,

$$P^k_{MD,i} = P(\sum_{j\in\mathcal{V}_i} \omega^d_{ij}\Theta^k_{ij} > \Gamma_k; \sum_{j\in\mathcal{V}_i} \delta^k_{ij} > 0), \tag{40}$$

$$P^k_{FA,i} = P(\sum_{j\in\mathcal{V}_i} \omega^d_{ij}\Theta^k_{ij} \leq \Gamma_k; \delta^k_{ij} = 0, j \in \mathcal{V}_i), \tag{41}$$

for $k \in \{u, d\}$. We ran the following steps, over 10^6 Monte Carlo simulations, to obtain the performance characteristics of the downlink IDS:

1) We set up the network such that $\delta^d_{1j} = 0 \; \forall j$.
2) In each iteration, M_1 vehicles obtain their respective individual trust value for R_1. We then calculate the aggregated trust value using these individual trust values.

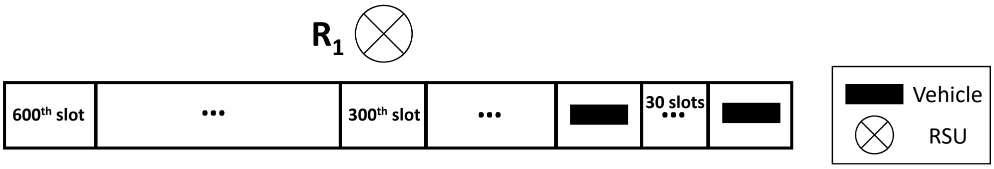

Fig. 4. Simulation model.

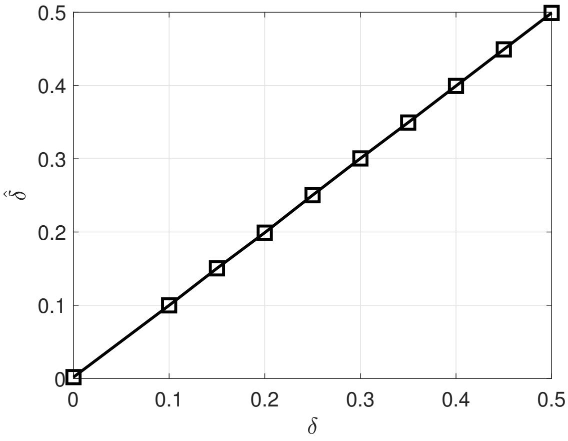

Fig. 5. Mean of the least square estimate.

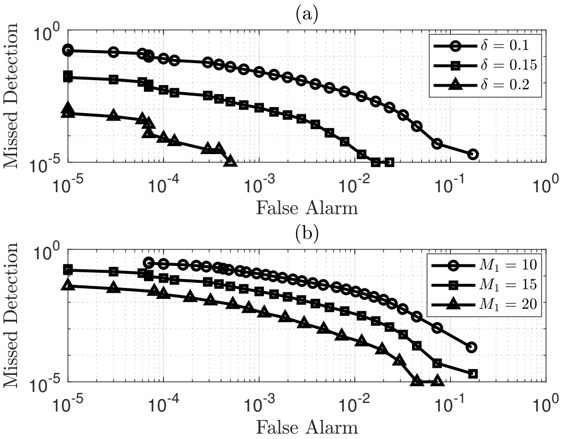

Fig. 6. Performance of the downlink IDS when (a) M_1 = 15 and the value of δ is varied (b) $\delta = 0.1$ and the value of M_1 is varied.

3) We then compared the above obtained aggregated trust value to a set of pre-defined threshold values to decide about the attack.

The simulated P_{FA}^{d} values are obtained by averaging over 10^6 Monte Carlo simulations. To obtain the simulated P_{MD}^{d} values, we set up the network such that $\delta_{1j}^{d} = \delta \; \forall j$ and follow the above approach. The results obtained for different values of M_1 and δ are plotted in Fig. 6. It can be seen from Fig. 6(a) that performance of the downlink IDS improves with increasing δ. Also, from Fig. 6(b), it can be observed that the performance improves with an increasing value of M_1.

We followed a similar procedure to obtain the performance characteristics of the uplink IDS. To obtain the value of P_{FA}^{u}, the values of $\delta_{ij}^{u}, j \in 1, \cdots, M_1$ are set to zero. To obtain the P_{MD}^{u} values, they are set to δ. The results obtained for different values of M_1 and δ are plotted in Fig. 7. It can be observed that the performance of the uplink IDS improves with increasing δ and M_1.

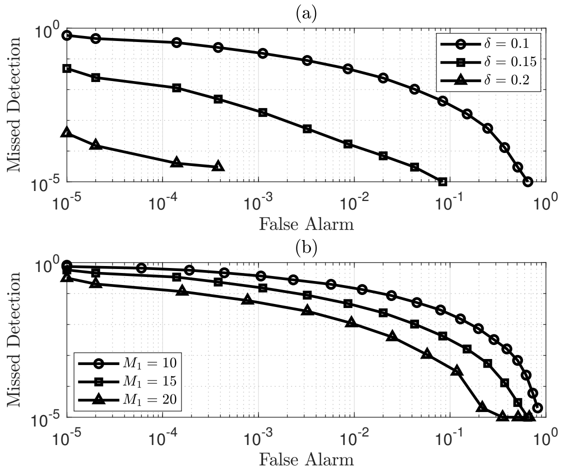

Fig. 7. Performance of the uplink IDS when (a) M = 15 and the value of δ is varied (b) $\delta = 0.1$ and the value of M is varied.

C. Performance in the Presence of Malicious Vehicles

In this section, we demonstrate the performance of the downlink and uplink IDSs in the presence of malicious vehicles. We consider a situation where RSU R_1 is benign and $M_1 = 25$. i.e., twenty five vehicles reported trust values (both uplink and downlink). The number of vehicles reporting false trust values is equal to M. Generally, in such a situation, the false alarm probability is used to evaluate the performance of the detection system. The false alarm probability is measured, over 10^6 Monte Carlo simulations, using the procedure described in Section VII-B. The only difference is that the M malicious vehicles obtain their respective individual trust values as described in Section VI. The results for different values of M and δ_v are plotted in Figs. 8 and 9, respectively. From both the figures, it can be observed that the false alarm probability increases as δ_v and/or M increase. However, the false alarm probability value remains negligible unless the value of δ_v is large and/or M is greater than the number of benign vehicles.

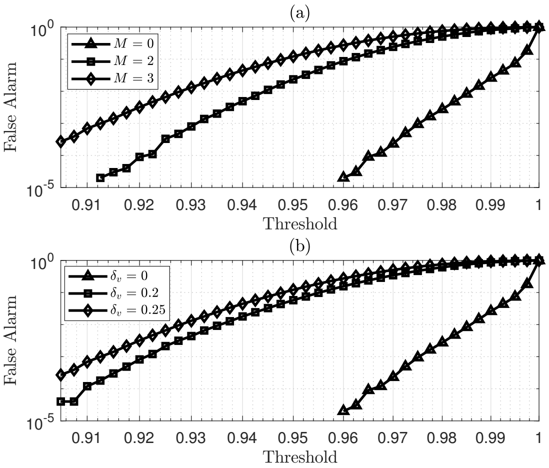

Fig. 8. Performance of the downlink IDS in the presence of malicious vehicles when (a) $\delta_v = 0.25$ and M is varied (b) $M = 3$ and δ_v is varied.

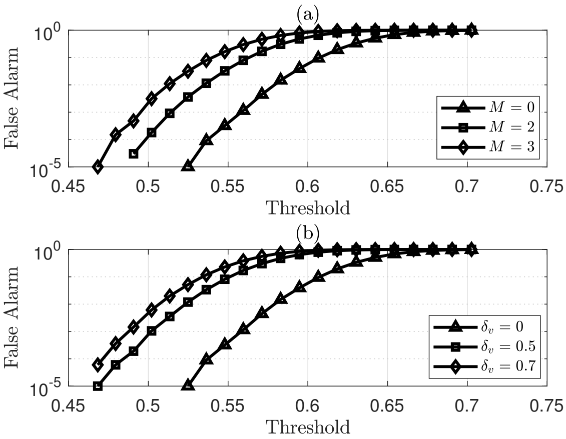

Fig. 9. Performance of the uplink IDS in the presence of malicious vehicles when (a) $\delta_v = 0.6$ and M is varied (b) $M = 3$ and δ_v is varied.

D. Malicious Vehicle Identification

Let's now consider a situation where twenty vehicles reported their individual trust values for ten benign RSUs. The number of vehicles reporting false trust values is $M = 3$. The performance of the Gaussian kernel (GK) based algorithms in (38) and (39) are characterized using false alarm and missed detection probabilities. We ran the following steps, over 10^5 Monte Carlo simulations, to obtain the false alarm probability:

1) The vehicles obtain their individual trust values for the 10 RSUs in each iteration, and then the aggregated trust value for all the RSUs is obtained.
2) We then use the trust values of a benign vehicle to obtain its similarity metric.
3) Then, we compare the similarity of the benign vehicle with a pre-defined threshold to decide if the vehicle is benign or malicious.

The missed detection probability values are obtained using a similar approach, with the only difference being that the similarity metric of a malicious vehicle is used. From the Figs. 10 and 11 it can be observed that the Gaussian Kernel-based similarity measure achieves almost equal to one detection probability.

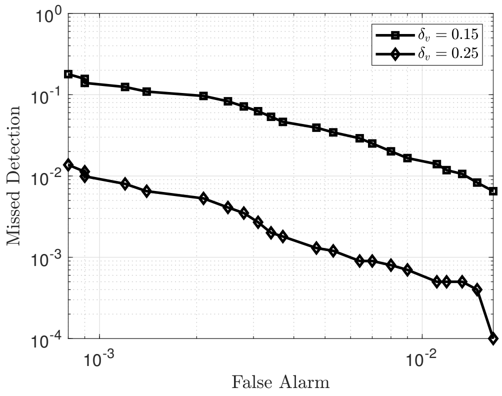

Fig. 10. Malicious vehicle identification on the downlink.

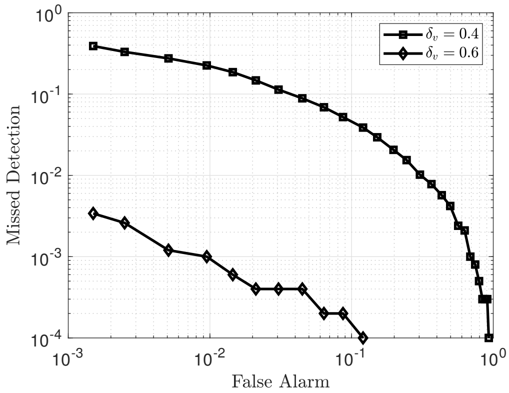

Fig. 11. Malicious vehicle identification on the uplink.

E. Comparison

The trust model presented in Section III-A is compared to the data-centric trust computation model described in [29].The individual trust (Θ^c_{ij}) of vehicle V_j towards R_i (for downlink) using the model in [29] can be computed as follows:

$$\Theta^c_{ij} = \frac{N^d_{ij}}{N^d_{ij} + \sum_k B^d_{ij,k}}. \tag{42}$$

The overall trust can be calculated using the procedure detailed in Section III-D. We follow the process in Section VII-B to obtain the performance characteristics, and the same are plotted in Fig. 12. We set $\delta_{ij} = \delta \ \forall j$. It can be seen that the IDS presented in this paper outperforms the Data-centric trust-based IDS for both the values of δ used. The trust value computed in (42) is calculated using the number of packets dropped by the vehicles. Therefore, the estimated trust value reflects the adversary's and the wireless channel's combined impact on the network. On the other hand, the trust value computed in Section III-D depends on the estimated attack probability and captures only the effect of the adversary on the network. The impact of the adversary can be seen distinctly

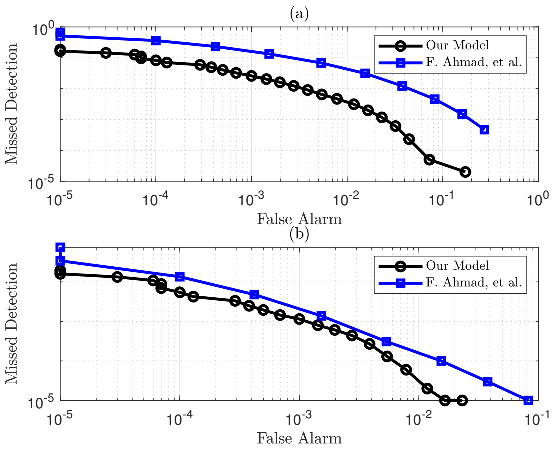

Fig. 12. Performance comparison of the IDSs for (a) $\delta = 0.1$ (b) $\delta = 0.15$.

in the trust calculated in this paper, i.e., in Section III-D as against to [29]. Therefore, we can achieve better performance.

VIII. Conclusion and Future Work

A. Conclusion

In this paper, trust-based IDSs are proposed to detect an adversary that has compromised an RSU, corrupting the communication between the RSU gateway and the vehicles. Firstly, the individual trust values are calculated by the vehicles and reported to the gateway. These values are then aggregated, using weighted sum, to obtain a single trust value for the RSU. The aggregated trust is then compared against a threshold to classify the RSU as benign or malicious. The packet drop probabilities of the packets received are used to determine the downlink trust values. The uplink trust values are calculated using the overall packet retransmission rate. The downlink trust value is obtained using the least square approach, and the uplink trust value is based on fuzzy logic. In addition, we also considered that there could be a small fraction of vehicles that report false trust values. A Gaussian kernel-based similarity metric is deployed to identify such vehicles. The similarity metric for a vehicle is calculated using the trust values reported by the vehicle about benign RSUs and the aggregated trust values of these RSUs. The similarity is then compared against a pre-defined threshold to classify if the vehicle is benign or malicious. The simulation findings show that malicious RSUs and malicious vehicles can be detected with a high degree of accuracy.

References

[1] P. Schulz *et al.*, "Latency critical IoT applications in 5G: Perspective on the design of radio interface and network architecture," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 70–78, Feb. 2017.

[2] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing - A key technology towards 5G," *ETSI White Paper no. 11*, 2015.

[3] B. Liang, V. W. S. Wong, R. Schober, D. W. K. Ng, and L.-C. Wang, "Mobile edge computing," in *Key technologies for 5G wireless systems*, Eds. Cambridge university press, 2017, pp. 1397–1411.

[4] P. Mach and Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1628–1656, 2017.

[5] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANET security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.

[6] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Netw.*, vol. 61, pp. 33–50, Jun. 2017.

[7] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, "Attacks on self-driving cars and their countermeasures: A survey," *IEEE Access*, vol. 8, pp. 207 308–207 342, Nov. 2020.

[8] M. Pham and K. Xiong, "A survey on security attacks and defense techniques for connected and autonomous vehicles," *Comput. Security*, p. 102269, Oct. 2021.

[9] P. K. Singh, S. Kumar Jha, S. K. Nandi, and S. Nandi, "Ml-based approach to detect DDoS attack in V2I communication under SDN architecture," in *Proc. IEEE TENCON*, Oct 2018.

[10] M. Chuang and J. Lee, "Ppas: A privacy preservation authentication scheme for vehicle-to-infrastructure communication networks," in *Proc. CECNet*, Apr. 2011.

[11] N. Ekedebe *et al.,* "On a simulation study of cyber attacks on vehicle-to-infrastructure communication (V2I) in intelligent transportation system (ITS)," in *Mobile Multimedia/Image Processing, Security, and Applications 2015*, Eds., vol. 9497, International Society for Optics and Photonics. SPIE, 2015, pp. 96–107.

[12] M. Amadeo *et al.*, "Securing the mobile edge through named data networking," in *Proc. IEEE WF-IoT*, 2018.

[13] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rogue AP detection," *IEEE Trans.Parallel Distrib. Syst.*, vol. 22, no. 11, pp. 1912–1925, Nov. 2011.

[14] F.-H. Hsu, Y.-L. Hsu, and C.-S. Wang, "A solution to detect the existence of a malicious rogue AP," *Comput. Commun.*, vol. 142, pp. 62–68, 2019.

[15] R. Jang, J. Kang, A. Mohaisen, and D. Nyang, "Catch me if you can: Rogue access point detection using intentional channel interference," *IEEE Trans. Mobile Comput.*, vol. 19, no. 5, pp. 1056–1071, 2019.

[16] N. S. Selvarathinam, A. K. Dhar, and S. Biswas, "Evil twin attack detection using discrete event systems in IEEE 802.11 Wi-Fi networks," in *Proc. IEEE MED*, 2019.

[17] P. Shrivastava, M. S. Jamal, and K. Kataoka, "Evilscout: Detection and mitigation of evil twin attack in SDN enabled WiFi," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 1, pp. 89–102, 2020.

[18] B. Li, T. Chen, and G. B. Giannakis, "Secure mobile edge computing in IoT via collaborative online learning," *arXiv preprint arXiv:1805.03591*, 2018.

[19] M. Hussain and B. M. Almourad, "Trust in mobile cloud computing with LTE-based deployment," in *Proc. IEEE ScalCom*, 2014.

[20] N. V. Abhishek, T. J. Lim, B. Sikdar, and B. Liang, "Detecting RSU misbehavior in vehicular edge computing," in *Proc. IEEE/CIC ICCC*, Aug. 2019.

[21] V. A. Nalam, T. J. Lim, B. Sikdar, and B. Liang, "Detecting selective modification in vehicular edge computing," in *Proc. IEEE VTC*, Sep. 2019.

[22] N. Baccour *et al.,* "Radio link quality estimation in wireless sensor networks: A survey," *ACM Trans. Sensor Netw.*, vol. 8, no. 4, p. 34, 2012.

[23] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels*. John Wiley & Sons, 2005.

[24] S. M. Kay, *Fundamentals of statistical signal processing, volume i: Estimation theory (v. 1)*. PTR Prentice-Hall, Englewood Cliffs, 1993.

[25] P. Victor, C. Cornelis, M. De Cock, and E. Herrera-Viedma, "Practical aggregation operators for gradual trust and distrust," *Fuzzy Sets Syst.*, vol. 184, no. 1, pp. 126–147, 2011.

[26] M. J. Wierman, "An introduction to the mathematics of uncertainty," *Creighton University*, 2010.

[27] J.-P. Vert and K. Tsuda, "A primer on kernel methods," *Kernel Methods Computational Biology*, vol. 47, pp. 35–70, 2004.

[28] P. Series, "Propagation data and prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 900 MHz to 100 GHz,". Recommendation ITU-R, 2012.

[29] F. Ahmad, A. Adnane, C. A. Kerrache, F. Kurugollu, and I. Phillips, "On the design, development and implementation of trust evaluation mechanism in vehicular networks," in *Proc. IEEE/ACS AICCSA*, 2019.

Nalam Venkata Abhishek (S'19 - M'21) received his Doctor from National University of Singapore in 2021 and Bachelor of Technology in Electrical Engineering from Indian Institute of Technology, Mandi, India, in 2014. Between 2014 and 2016, he worked in the industry where he was working towards developing efficient cellular and wireless technology solutions. Nalam is currently a lecturer in the Infocomm Technology cluster at Singapore Institute of Technology (SIT), Singapore. His research interests include wireless networks and security and machine learning for networks.

Teng Joon (T. J.) Lim (S'92-M'95-SM'02-F'17) obtained the B.Eng. degree in Electrical Engineering with first-class honours from the National University of Singapore (NUS) in 1992, and the Ph.D. degree from the University of Cambridge in 1996. From September 1995 to November 2000, he was a Researcher at the Centre for Wireless Communications in Singapore, one of the predecessors of the Institute for Infocomm Research (I2R). From December 2000 to May 2011, he was Assistant Professor, Associate Professor, then Professor at the University of Toronto's Edward S. Rogers Sr. Department of Electrical and Computer Engineering. From June 2011 to January 2020, he was a Professor at the Electrical & Computer Engineering Department of NUS, where he served as a Deputy Head from July 2014 to August 2015. From September 2015 through December 2019, he served as Vice-Dean (Graduate Programs) in the NUS Faculty of Engineering. Since January 2020, he has been Deputy Dean and Associate Dean (Education) at the Faculty of Engineering in the University of Sydney. Professor Lim is an Associate Editor for IEEE Potentials, was an Area Editor of the IEEE Transactions on Wireless Communications from September 2013 to September 2018, and previously served as an Associate Editor for the same journal. He has also served as an Associate Editor for IEEE Wireless Communications Letters, Wiley Transactions on Emerging Telecommunications Technologies (ETT), IEEE Signal Processing Letters and IEEE Transactions on Vehicular Technology. He has volunteered on the organizing committee of a number of IEEE conferences, including serving as the TPC co-chair of IEEE Globecom 2017. He chaired the Singapore chapter of the IEEE Communications Society in 2017 and 2018 and was a Distinguished Lecturer of the IEEE Vehicular Technology Society for 2019-20. He was a Co-winner of the IEEE Communications Society's 2020 Heinrich Hertz Award for Best Communication Letter. His research interests span many topics within wireless communications, including cyber-security in the Internet of Things, heterogeneous networks, cooperative transmission, energy-optimized communication networks, multi-carrier modulation, MIMO, and stochastic geometry for wireless networks, and he has published widely in these areas.