Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection

Kamran Zaidi, Milos B. Milojevic, *Student Member, IEEE*, Veselin Rakocevic, *Member, IEEE*, Arumugam Nallanathan, *Senior Member, IEEE*, and Muttukrishnan Rajarajan, *Senior Member, IEEE*

***Abstract*—In this paper, an intrusion detection system (IDS) for vehicular ad hoc networks (VANETs) is proposed and evaluated. The IDS is evaluated by simulation in the presence of rogue nodes (RNs) that can launch different attacks. The proposed IDS is capable of detecting a false information attack using statistical techniques effectively and can also detect other types of attacks. First, the theory and implementation of the VANET model that is used to train the IDS is discussed. Then, an extensive simulation and analysis of our model under different traffic conditions is conducted to identify the effects of these parameters in VANETs. In addition, the extensive data gathered in the simulations are presented using graphical and statistical techniques. Moreover, RNs are introduced in the network, and an algorithm is presented to detect these RNs. Finally, we evaluate our system and observe that the proposed application-layer IDS based on a cooperative information exchange mechanism is better for dynamic and fast-moving networks such as VANETs, as compared with other techniques available.**

***Index Terms*—Cryptography, fault tolerance, intrusion detection, rogue nodes (RNs), security, vehicular ad hoc networks (VANETs), vehicular networks, wireless networks.**

I. Introduction

VEHICULAR ad hoc networks (VANETs) are considered to be the next big thing that will change our lives remarkably. It is only logical that technology is used to make our lives and roads safer. Currently, the automotive industry looks all set to equip vehicles with wireless access vehicular environment (WAVE) devices, which will enable vehicles to communicate with each other to exchange safety information. Moreover, autonomous vehicles are not that far off either, with Google Car a reality today. These technological innovations in our vehicles will change the way we think about road travel by making it much safer and productive. WAVE protocols are based on the IEEE 802.11p standard and provide the basic radio standard for dedicated short-range communication (DSRC) in VANETs. Vehicles use DSRC to communicate with each other, i.e., vehicle to vehicle (V2V), and with the infrastructure (road side units—RSUs), i.e., vehicle-to-infrastructure communication.

VANETs will become a reality in the very near future. The tremendous safety, convenience, and commercial potential of vehicular networks will not only drive their deployment but will also be fuelled by their demand once consumers realize their effectiveness. VANETs have the ability to make roads safer, particularly in conditions that are currently considered hazardous and unavoidable. Imagine the ability to be able to navigate safely under otherwise very dangerous driving conditions such as fog, accidents, and black ice. However, there are some very serious security issues that need to be addressed before the full potential of VANETs can be realized. Vehicular networks are very fast moving and highly dynamic, due to which it is very important that the information being shared is authentic and actionable. As encounters will be short lived and the received information has to be actioned quickly, it is important that the reliability of the information is ascertained quickly.

In ad hoc networks, maintaining and depending on trust or reputation is a very expensive and complex concept. In VANETs, centralized trust has long been debated as it is difficult to maintain, update, and use. The existing mechanism for authenticating messages in vehicular networks involves the use of cryptography [7]–[9] and trust [18]–[20]. Cryptographic techniques involve paired keys and overhead in terms of computing cost, storage, and time. Even with cryptographic techniques, security lapses are inevitable, leading to intrusions due to stolen keys or compromised trusted authorities, etc. An attack is particularly difficult to prevent when it is launched from within the network. Due to the wireless and mobile nature of vehicular networks and their dynamic topology, it is not possible to use the same intrusion detection mechanisms that are used in wired networks. Therefore, it is essential that an intrusion detection system (IDS) is deployed to detect attacks and help secure VANETs. The proposed IDS will detect different types of attacks launched by rogue or compromised nodes in the network. The IDS will then be able to minimize the damage to the network by taking necessary actions. The proposed IDS works in a distributed manner and is designed for deployment at each host node in the vehicular network.

A. Our Contributions

The main contributions in this paper are given in the following.

1) An IDS is proposed that uses statistical techniques to detect anomalies and identify rogue nodes (RNs) using

Manuscript received March 5, 2015; revised July 16, 2015; accepted September 12, 2015. Date of publication September 18, 2015; date of current version August 11, 2016. The review of this paper was coordinated by Prof. Y. Zhang.

K. Zaidi, M. B. Milojevic, V. Rakocevic, and M. Rajarajan are with the School of Mathematics, Computer Science and Engineering, City University London, London EC1V 0HB, U.K. (e-mail: kamran.zaidi.1@city.ac.uk; milos.milojevic.1@city.ac.uk; veselin.rakocevic.1@city.ac.uk; r.muttukrishnan@city.ac.uk).

A. Nallanathan is with the Department of Informatics, King's College London, University of London, London WC2R 2LS, U.K. (e-mail: arumugam.nallanathan@kcl.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2015.2480244

a traffic model. We significantly extend the earlier work done in [23] by extensive simulations under varying vehicular and network traffic conditions and using statistical techniques to determine false data, particularly in emergency messages.

2) The extensive data collected are analyzed using statistical techniques, and the decision to accept or reject data is based on hypothesis testing.
3) The effects of various parameters such as transmission intervals and vehicle density are also shown.
4) The proposed IDS is not dependent on any infrastructure, such as RSU, or expensive hardware, such as lidar, radar, or cameras.
5) Using the proposed mechanism, network message congestion is controlled by reduced message transmissions, which prevent broadcast storms. Moreover, we show that using the proposed model and IDS, it is possible for vehicles to keep the network functioning even when up to 40% of nodes are malicious and contribute false parameter values.

The rest of this paper is organized as follows: Related work is discussed in Section II. The system and the attack model are presented in Section III. In Section IV, an overview of the proposed IDS is presented. Section V evaluates the security performance of the proposed IDS in detail. Results are discussed in Section VI, and the conclusion and future work are given in Section VII.

II. Related Work

Security of VANETs is a very important issue and has been the focus of research for many years. The vehicular networks are unique as the users will be making life-saving decisions based on the information being received. It is therefore imperative that there is a mechanism to detect false information. Researchers have proposed using cryptography and digital signatures to secure and sign messages to ensure integrity and nonrepudiation of messages in VANETs. Digital signatures have been proposed for VANETs in [4]–[6]. Different schemes have been proposed, including public key infrastructure [7]–[9].

The propagation of emergency messages in VANETs is done either through multihop or by broadcasting them. Therefore, malicious behavior, e.g., false information attack, is possible, even in case of strong cryptography as insiders can turn malicious. A malicious user might send false alert to clear the road for himself or cause havoc by creating a traffic jam by sending a fake accident alert. In [13], using data-centric techniques to make VANETs more reliable by only considering the data being shared has been suggested. For fast-moving and dynamic networks, information-centric schemes are required, in addition to the cryptography and certificates, to protect against inside attacks.

There are mainly two approaches to deal with the false information attacks, i.e., trust- or reputation-based schemes and data-centric schemes. This trust based on reputation can either be infrastructure based or self-organizing [17]. Self-organizing trust means to assign a trust score to another user based on previous or current interactions. This trust score represents the reputation of the user in the network and helps other nodes decide whether it can be trusted or not. Such voting schemes (credit scores) are promising in wired networks or online systems where the users have a fixed physical identity, but they are difficult to implement in a fast-moving and rapidly changing network such as VANETs. Reputation-based schemes have been proposed in [18]–[20]. In [19] and [20], a decentralized infrastructure has been adopted, whereas in [18], a centralized infrastructure is proposed. Reputation- and trust-based schemes are useful but cannot be used to detect false emergency messages as trust is built over a period of time, and if a false message comes from a trusted node, then there is no way to detect it.

Data-centric misbehavior detection techniques have been proposed in [15] and [18]. In [18], a model of VANETs to be used to detect and correct errors in the data being sent out by vehicles is proposed. The messages that conform to the model are accepted, and rejected otherwise. In [15], emergency messages are relayed, and false information is identified based on the kind of message and the subsequent behavior of the sending vehicle. Such a technique will not be feasible for emergency messages that need to be acted on quickly. In addition, such a scheme will increase the computation cost for the nodes. A misbehavior detection system and eviction mechanism is proposed in [16], where nodes are termed misbehaving if their information is inconsistent with the situation. Once a node is classified as a misbehaving node, then the neighboring nodes can temporarily evict it by sharing warning messages about it, and later, its credentials are passed on to the certificate authority (CA), which revokes them by adding them to a revocation list (RL). However, as previously discussed, the RLs are difficult to manage and use in VANETs.

Intrusion detection is the most reliable approach to protect vehicular networks against threats as it has the ability to detect insider and external attacks with high accuracy [2]. Some research has been done in the area of IDS/intrusion prediction system (IPS) for mobile ad hoc networks (MANETs) and VANETs in [1] and [24]–[30]. In [26], an acknowledgement scheme to prevent packet dropping and false misbehavior report generation by nodes for MANETs to report or convict an RN is proposed. In [27], a watchdog for intrusion detection in VANETs is proposed. The watchdog works by monitoring all packets to decide if an attack is under progress. In [25], trust and position information are combined to determine if a vehicle is falsifying its position, i.e., if the position claimed by one vehicle overlaps the position claimed by another, in which case the vehicle with the lower trust value is flagged as an intruder. In [24], a method is proposed to detect intrusions through trust by assigning reputation scores to vehicles, and the RSUs are used to compute these scores and the CA aggregates them. Similarly, in [1], rule-based anomaly detection and reputation scores are used for the IDS in the vehicular network. In [28] and [29], intrusion prediction approaches have been discussed.

IDSs are very effective as they are able to detect attacks from insiders at real time but, at the same time, need to be updated for new attacks. Moreover, IDSs need strong authentication and identification systems to work properly. IPSs, on the other hand, try to predict new attacks that can protect the system from

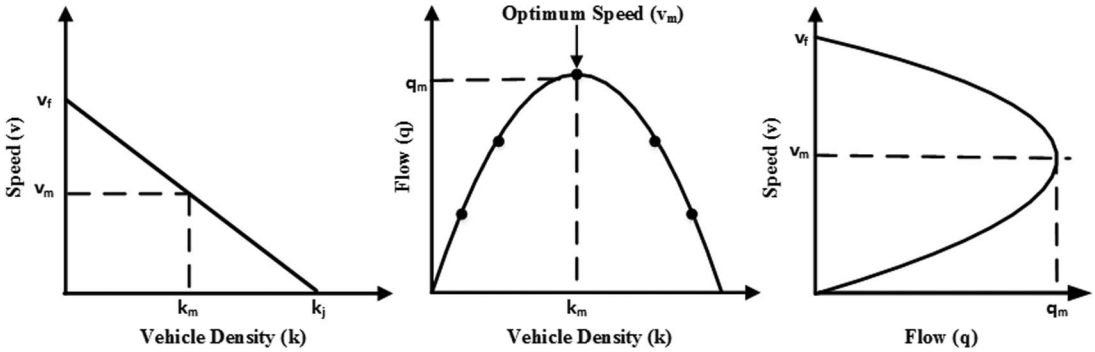

Fig. 1. Greenshield's fundamental diagrams. (a) Speed versus vehicle density. (b) Flow versus vehicle density. (c) Speed versus flow.

unknown attacks. However, the probability thresholds need to be set carefully in such IPSs to get accurate results. This work proposes an IDS that does not use trust or reputation and only relies on the analysis of the received data to detect intrusions in the network. The statistical technique used in the IDS declares if the data are true or false, which leads to the node being declared honest or rogue instead of the other way around.

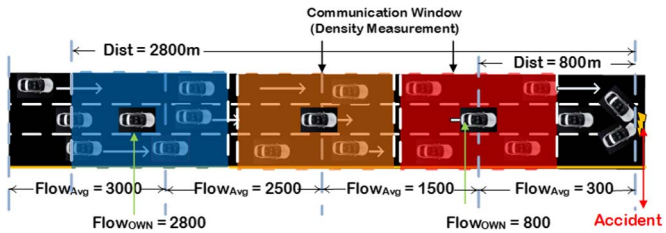

Fig. 2. Decreasing value of flow in case of an accident.

III. Preliminaries

A. Authentication and Privacy Preservation

In any network, it is very important that nodes can be identified correctly and are distinguishable from one another but, at the same time, privacy is preserved. This means that all nodes are authenticated by a CA. It is assumed that all vehicles have authenticated themselves with a CA and obtained a valid certificate and public/private key pairs (Pseudonyms—PNs). The keys are used to encrypt the routine messages, and others can authenticate and decrypt the messages by using the relevant public keys. It is also assumed that all vehicles have enough key pairs to last them a long time, and they keep changing these keys to preserve their privacy. However, these keys are changed in a reasonable time, i.e., not too quickly, to avoid short-term linkability. This ensures that, even by changing PNs, the recent messages of a node can be linked to the same node. Therefore, the proposed IDS allows the nodes to change their PNs but can still keep track of the RNs.

B. VANET Model

To model the flow of traffic on motorways/highways, a mathematical model is needed. Therefore, Greenshield's model, which is considered to be a fairly accurate model in traffic engineering to estimate and model uninterrupted traffic (without traffic signals), is utilized. Greenshield's model uses standard parameters such as flow (vehicles per hour) and density (vehicles per kilometer). The model describes the relationship between speed v and density k of vehicles as being negatively correlated, with density increasing with the decrease in speed, as shown in Fig. 1(c). In the figure, v_f is the free-flow speed when density is zero, i.e., vehicles can choose to move freely as there are no or very few vehicles on the road. As the density of vehicles increases, the speed decreases until density reaches the maximum, which is referred to as jam density or k_j, at which point the speed becomes zero and vehicles are stuck in a traffic jam. In the figure, k_m and v_m are the optimal density and speed, respectively, which allows the traffic to progress at the optimum rate of flow, i.e., q_m [see Fig. 1(a)–(c)]. The flow is given as

$$q = k \times v. \tag{1}$$

The relationship between speed and density is given as

$$v = v_f - \frac{k}{k_j} v_f. \tag{2}$$

From (1) and (2), the relationship between speed and density can be found to be

$$q = v_f k - \frac{k^2}{k_j} v_f. \tag{3}$$

Each vehicle can calculate the density of vehicles on the highway around it by the number of messages it receives from other vehicles by checking their IDs from messages. This enables each vehicle to calculate the density quite accurately in a moving window around itself, as shown in Fig. 2. The size of this density window is equal to the transmission and reception range of a vehicle (500 m). This means that a vehicle can receive messages from a vehicle that is up to 500 m ahead of it and 500 m behind it. Therefore, each vehicle has a communication window of 1000 m around it that it can use to calculate the density $\text{Density}_{\text{calc}}$. In addition, each vehicle can calculate the average speed of vehicles $\text{Speed}_{\text{AVG}}$ within its communication window. In our scheme, each vehicle transmits not only its location and speed but the calculated value of flow as well. Therefore, the vehicles calculate the traffic flow parameter using density and average speed of other vehicles through

Greenshield's model. The flow serves as a global parameter that each vehicle calculates on its own and should be very similar for vehicles that are close to each other under the same traffic conditions. Moreover, information will be considered correct if it conforms to this model and false otherwise.

The idea behind this mechanism is that, in case of an emergency (an accident or sudden braking), all vehicles behind the incident will apply brakes, and therefore, their flow values will go down. These low values of flow will be transmitted to other vehicles behind them, which will cause their calculated flow values to go down as well, as shown in Fig. 2. The red region is where the brakes have been applied, and the orange region is where the effect information is being propagated and where vehicles are getting information of an accident up ahead. The blue region is some distance away where vehicles are getting reports of some congestion ahead on the highway but they do not have to start braking just yet. This is one of the benefits and desirable effects of the proposed model, as there is no need to flood the network with the congestion warning, and instead, the information is propagated gracefully. However, in case of a false emergency message, a vehicle will try to create the illusion of an accident by lowering its flow and speed values and transmitting it to others. However, as there is only one vehicle that is transmitting this low value, it can easily be flagged and identified.

Each vehicle transmits its Flow_{AVG}, which becomes $\text{Flow}_{\text{RCVD}}$ for other vehicles. If a vehicle receives a value of flow from another vehicle that does not agree with the VANET model, then the data are rejected, and vehicles' ID is noted and reported. If the data agree with the model, then the receiving node checks the data with its own calculated values to confirm if its values are indeed correct. If the values do not agree with the node's own calculated parameters of flow, speed, and density, then the values are discarded, and the sender ID is reported. The two values of flow are calculated as follows:

$$\text{Flow}_{\text{OWN}} = \text{Speed}_{\text{AVG}} \times \text{Density}_{\text{calc}} \tag{4}$$

$$\text{Flow}_{\text{AVG}} = \frac{1}{n}\sum^{n} \text{Flow}_{\text{RCVD}}. \tag{5}$$

C. Message Format

Each vehicle creates its own message m for beacon, and apart from the usual parameters, it also includes the following:

$$m(\text{Speed}_{\text{Own}}, \text{Density}_{\text{calc}}, \text{Flow}_{\text{AVG}}).$$

Each beacon message m is hashed $(H(m))$ and signed by the vehicle using its secret key (SK), i.e.,

$$\text{sig} = \text{SK}(H(m)).$$

The details of how this signature is generated and how they are verified are not in the scope of this paper. In case of an emergency, e.g., an accident or emergency braking, each vehicle generates an emergency message, which has the following format:

$$\text{Emergency Msg}(\text{Type}, \text{Flow}_{\text{AVG}}, \text{Speed}_{\text{Own}}, \text{Density}_{\text{calc}})$$

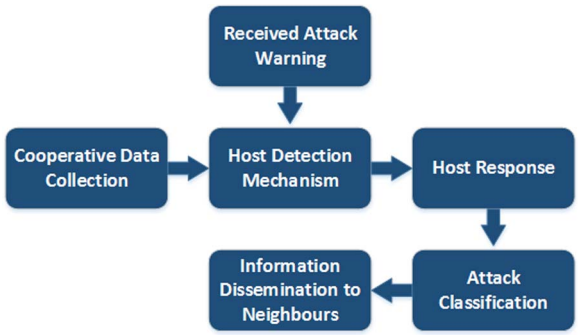

Fig. 3. Proposed host-based IDS.

where the field Type can be emergency braking, accident ahead, slippery road, etc. It must be noted that the emergency messages are not encrypted and have to be actioned quickly by those receiving them.

D. Attack Model

There are different types of attacks that can take place in VANETs. We will be looking at the following attacks.

1) *False information attack*: An RN can inject false data in the network either on purpose with malicious intent or due to faulty sensors, which can cause serious damage to the network. Under extreme conditions, the network can even be paralyzed. The RN can start injecting false data at any time and can falsify values of their own speed and their calculated values of flow and density in either beacon message or emergency message. In case of a false emergency message, the RN will start sending a low value of flow or a sudden decrease in speed, or both, to indicate an accident or emergency braking.
2) *Sybil attack*: Another attack that an RN can launch is a Sybil attack, i.e., when a rogue vehicle transmits multiple messages, each with a different ID, to indicate that it is not one vehicle but many vehicles, thereby giving a false impression of congestion by lowering the flow values in the messages. The IDs could have been either spoofed or stolen from compromised nodes.

IV. Intrusion Detection System Overview

The host-based IDS proposed in this paper is deployed at each vehicle and is able to detect intrusions in VANETs and then take corrective measures to contain the damage. To train the IDS, a model of the network under normal conditions is needed, so that deviations (anomalies) from the normal behavior can be detected and alarms can be raised, i.e., other vehicles can be informed (see Fig. 3). In the proposed model discussed in the previous section, the vehicles send their speed, calculated average flow, calculated density, and location information to other vehicles. In addition, each vehicle calculates its own value of average flow, which provides the vehicle with a very good estimate of the traffic in its vicinity and up ahead as well.

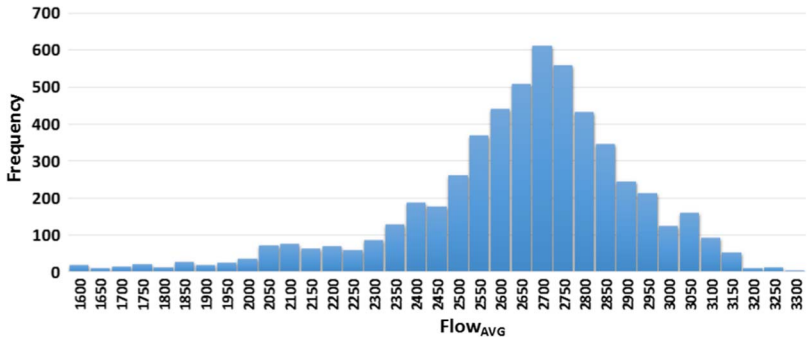

Fig. 4. Flow_{AVG} values for Node 90 between $t = 203$ s and $t = 325$ s.

A. Cooperative Data Collection

Using our scheme, each node (vehicle) collects data from other nodes (vehicles) in its vicinity to model the traffic around it. The vehicles cooperate with each other and share the values of their parameters using the Greenshield's model described earlier. As a vehicle will receive the parameter values from all other vehicles within the range, each vehicle has information about all the vehicles in that region. Due to this, each vehicle can calculate the (estimate) mean μ. The trace data have shown that, under all conditions, the flow values will be close together and will lie within two standard deviations of the mean. This means that all vehicles that are within the communication range are calculating very similar values of the Flow_{AVG} as they are under similar traffic conditions. This is obvious as all nodes are dependent on other nodes to calculate their parameter values in all circumstances, i.e., free-flowing traffic and in case of an accident. When enough readings/data have been gathered, the conditions of the central limit theorem apply, and we approach a normal distribution. To show this, we plot the frequency distribution of the average flow values Flow_{AVG} of a random node, e.g., Node 90 in our simulation with vehicle inter-arrival time of 2 s, transmission interval of 0.5 s from simulation time $t = 203$ s to $t = 325$ s, as shown in Fig. 4. The data are slightly left skewed as vehicles start from rest and therefore have lower values of flow in the beginning. This means that we are now in a position to set up a hypothesis test and use the t-test for detecting false values reported by a rogue/malicious vehicle. The t-test for comparing the two population means is used, as the sample size can be small.

The parameter values follow a normal distribution, and as the received values are in pairs, we use the paired t-test to calculate the probabilities associated with getting values in different ranges. The standard deviation and the test statistic t_o are calculated as

$$t_o = \frac{\bar{x} - \bar{y}}{\sqrt{\frac{s_x^2}{n_1} + \frac{s_y^2}{n_2}}}. \tag{6}$$

Here, $\bar{x}$ is the mean difference of the received values, and $\bar{y}$ is the mean difference of the vehicle's own calculated values; s_x and s_y are the standard deviations of the received and vehicle's own calculated values, respectively. n_1 and n_2 are the number of samples for the received and own values, respectively. The degrees of freedom will be $n_1 + n_2 - 2$. The algorithm of the proposed IDS is given in Algorithm 1. The data are collected from all neighboring nodes and checked if there is a significant difference between calculated and received values. If there is a significant difference, then the node is monitored, and some parameter values are collected (accepted) initially. Once sufficient samples have been collected, then the t-test is carried out. If the t-test gives a result within the acceptance region, then the data are accepted and else rejected. If the data are rejected, then the node is highlighted as rogue, the attack is classified as an information attack, and subsequent values from that node are rejected. A message is then sent to other users, informing them of the RN and the type of attack being launched by that node.

Algorithm 1 Algorithm for IDS

```
for each msg received do
    Update Density_calc
    Update Speed_AVG
    Flow_OWN = Speed_AVG × Density_calc
    if Flow_RCVD − Flow_OWN < Threshold then
        Accept Data
        Calculate Flow_AVG
    else
        Monitor Node and Accept Data temporarily
        if Hypothesis Test == Reject then
            Reject Data
            Report Node
            Calculate Flow_AVG
        end if
    end if
end for
```

B. Hypothesis Testing for Data Correctness

Hypothesis testing is a common technique used in engineering applications to test two claims when only one of them can be true. The hypothesis testing approach also assigns a confidence interval to a range of values that enables us to accept a claim with a certain confidence. This suits us, as in our VANET model and the proposed IDS, there are two possibilities, i.e., either the node is honest and we accept its data, or the node is

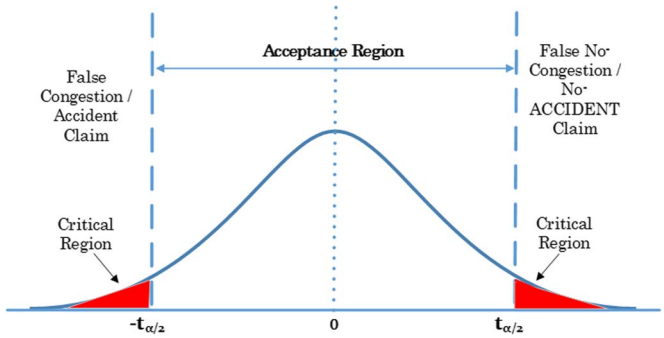

Fig. 5. Distribution of t_o for Flow_{AVG}.

TABLE I
DECISIONS IN HYPOTHESIS TESTING

	Node is Honest - H_o	Node is Rogue - H_a
Accept H_o	No Error	Type 2 Error
Reject H_o	Type 1 Error	No Error

rogue and we reject its data. To check whether hypothesis testing works well in our model, we ran the simulations numerous times in OMNET++ and then exported the data to MS Excel and MATLAB to analyze and visualize them.

We use hypothesis testing to decide whether a received parameter value should be accepted or not. If the received value is within the 99% confidence interval, i.e., within the acceptance region, then the value is accepted. If the received flow value is within the rejection region, then it is rejected. This is shown in Fig. 5. There are always two hypotheses stated: There is the null hypothesis H_o that we want to test (and assumed to be correct) and the alternate hypothesis H_a. If the null hypothesis is rejected, then the alternate hypothesis is accepted, and if we do not have enough evidence against the null hypothesis, then it is accepted. The null hypothesis H_o in our case is that the flow value received is from an honest node (HN). The alternate hypothesis H_a is that the value received is false (from an RN), and we fail to accept (reject) it. In other words, we say that we do not have enough evidence to accept the received value, and therefore, we reject it. The hypotheses that will be tested in the host IDSs are stated as follows:

H_o : Accept Received data (Node is Honest)

H_a : Reject (Fail to Accept) Received data (Data is false & Node is Malicious or Rogue).

The IDS in each vehicle also computes a p-value that helps it in accepting or rejecting the null hypothesis. The p-value gives the probability of getting a value that is at least as extreme as the one that was observed; therefore, the p-value gives information about the weight of evidence against the null hypothesis H_o, i.e., the smaller the p-value, the greater the evidence against H_o. There are two types of errors associated with hypothesis testing, as shown in Table I. In our scenario, a Type-2 error (false negative) is not very serious, as the worst-case scenario is slowing down, whereas a Type-1 error (false positive, FP) is very serious. Therefore, keeping this in view, we use a wide confidence interval. The level of significance is denoted by α. The usual values of α are taken to be 0.01(1%) or 0.05(5%), which means the probability that the test statistic falls in our acceptance region is $1-\alpha$ and the confidence intervals for the two values of $\alpha = 0.01$ and 0.05 are 99% and 95%, respectively. We take the value of α to be 0.01, and as this will be a two-tailed test, the upper and lower limits of our acceptance region will be $t_{\alpha/2}$ and $-t_{\alpha/2}$, as shown in Fig. 5. The degrees of freedom will be $n_1 + n_2 - 2$, and the corresponding limits can be looked up from the t-table. This means that the probability is α when the test statistic t_o falls in the region $t_o > t_{\alpha/2}$ or $t_o < -t_{\alpha/2}$ when the null hypothesis H_o is true. Therefore, we will reject the received value if it is outside the acceptance region, i.e., we reject the value if either

$$-t_{\frac{\alpha}{2}} > t_o > t_{\frac{\alpha}{2}}.$$

In our case, the received flow values for any chosen node are always within the acceptance region or within the 99% confidence interval, as long as the node is honest. In case of an accident, as the values will drop, they will have an impact on all vehicles in the region, which will decrease the Flow_{AVG} value for the region, and as a result, the values are still within the acceptance region as the standard deviation increases.

As shown in Fig. 5, there are two cases where the RN will falsify its values, i.e., it can either deny congestion or accident or it can wrongly give the impression of congestion or accident. Therefore, the IDS can decide which category the false information falls under depending on whether $t_o > t_{\alpha/2}$ or $t_o < -t_{\alpha/2}$.

TABLE II
SIMULATION PARAMETERS

PARAMETER	VALUE
Simulation Time	400 sec
Scenario	3 Lane Highway
Highway Length	5-Kms
Max Vehicle Speed	28 m/sec or 100 Km/hr
Mobility Tool	VACaMobil
Network Simulation Package	OMNET++
Vehicular Traffic Generation Tool	SUMO
Vehicle Inter-Arrival Rate	1s, 2s and 3s
Transmission Rate	Every 0.2s, 0.5s and 1s
Wireless Protocol	802.11p
Transmission Range	500m in each direction

V. PERFORMANCE EVALUATION

A. Simulation Setup

To check the proposed IDS, extensive simulations were done using OMNET++, Simulation of Urban Mobility (SUMO) [22], and VACaMobil [21]. OMNET is a modular C++ library and framework that is used for network simulations. SUMO is a software tool that is used to generate vehicular traffic by specifying speed, types, behavior, and number of vehicles. SUMO also sets up road types and conditions. VACaMobil is a car mobility manager for OMNET that works in parallel with SUMO.

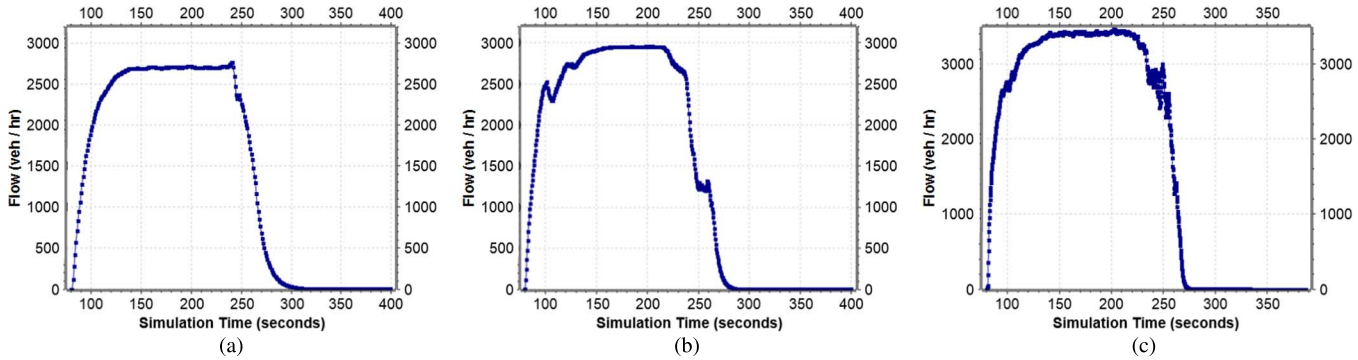

Fig. 6. Accident scenario: Inter-arrival time = 1 s. All vehicles start at approximately $t = 80$ s. (a) Node 50, update interval 1 s. (b) Node 59, update interval 0.5 s. (c) Node 56, update interval 0.2 s.

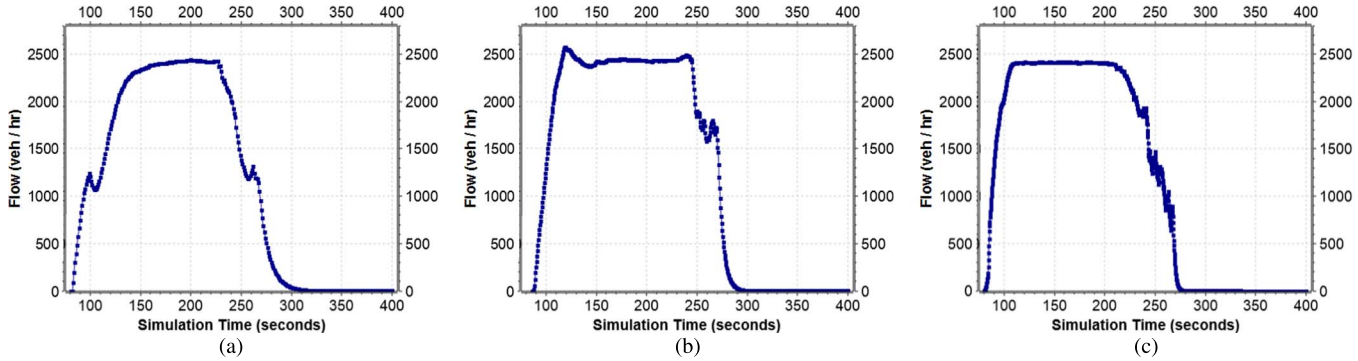

Fig. 7. Accident scenario: Inter-arrival time = 2 s. All vehicles start at approximately $t = 80$ s. (a) Node 39, update interval 1 s. (b) Node 40, update interval 0.5 s. (c) Node 36, update interval 0.2 s.

The scenario is simulated with parameters shown in Table II. To gather data for anomaly detection, we use different scenarios. We gather data when there is no accident and no RNs to understand and develop the model under normal circumstances. Data are also collected for runs in case of an actual accident to understand how parameters will change. Furthermore, RNs are inserted in both cases, i.e., in case of normal conditions (no accident) and in case of an actual accident, to see how well our IDS works. The simulations are carried out with varying values of the following parameters.

1) ***Density***: The density of nodes is an important parameter for ad hoc networks, particularly for VANETs. As the channel bandwidth is limited, it is essential to keep it under consideration and observe its effects on any system. In this paper, we vary the density of vehicles by changing their inter-arrival time, i.e., the time that they are inserted in the simulation. We use OMNET's exponential inter-arrival distribution with time periods of 1, 2, and 3 s.
2) ***Beaconing rate or sampling rate***: This is the beaconing time period after which each vehicle is transmitting its parameters to other vehicles. We have used variable time periods to observe the effects of this on VANETs, in general, and the proposed IDS, in particular. We have used time periods of 0.2, 0.5, and 1 s. It is worth mentioning that the recommended beaconing rate in IEEE 809.11p is 100 ms (0.1 s). The minimum time period of 0.2 s was chosen, as the generated data set was becoming too large, and data processing was becoming a problem.
3) ***Number of RNs***: The number of RNs is varied to evaluate the performance of the proposed scheme and the IDS in these circumstances.

A large amount of trace data are generated with the simulation runs by the varying parameters described earlier. For example, the maximum data generated and collected in this paper in one simulation, when the sampling rate is 0.2 s, the total number of vehicles that are active in simulation in case of an accident is 300, and the simulation time is 400 s, are more than 18 000 data points, out of which around 10 000 are vectors. The minimum data generated in one simulation, when the sampling rate is 1 s, the total number of vehicles that are active in simulation in case of no accident is around 150, and the simulation time is 400 s are around 10 000 data points, out of which around 6000 are vectors. The parameters of interest from the large data set were exported to MS Excel and MATLAB for analysis, testing, and visualization.

B. Simulation Results

1) Actual Accident Scenario—No Rogue Nodes: The results for the actual accident scenario are shown in Figs. 6–8. The density of vehicles (controlled by inter-arrival time) and the update interval (transmission rate) are varied in the simulations to study their effects. What is noteworthy here is that the flow parameter gradually decreases, which proves our earlier assumption.

In Fig. 6(a)–(c) the results are shown for the value of Flow_{AVG} for vehicles that start at approximately $t = 80$ s, and

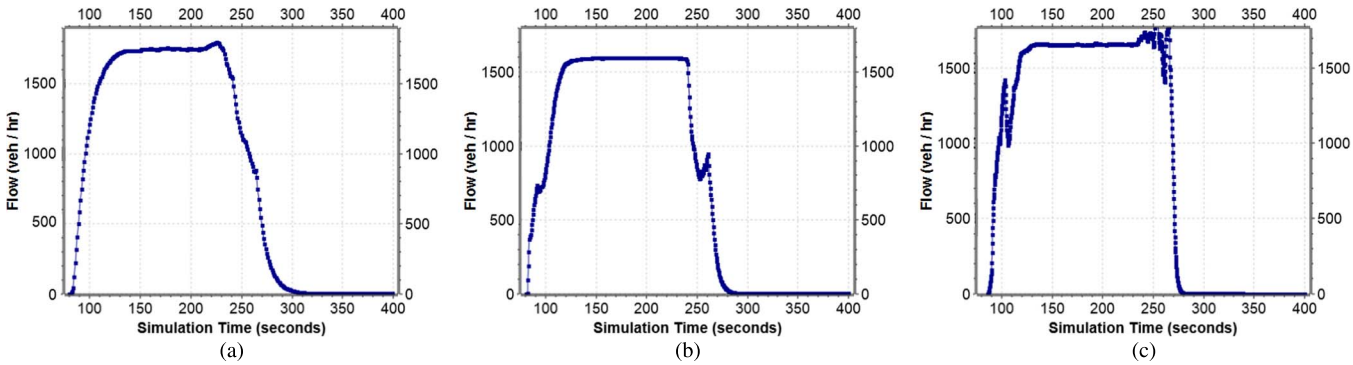

Fig. 8. Accident scenario: Inter-arrival time = 3 s. All vehicles start at approximately $t = 80$ s. (a) Node 32, update interval 1 s. (b) Node 26, update interval 0.5 s. (c) Node 24, update interval 0.2 s.

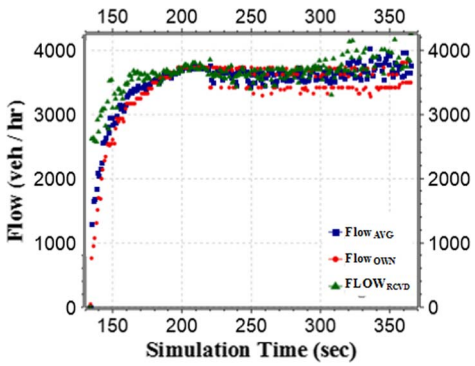

Fig. 9. Distribution of Flow_{AVG}, Flow_{OWN}, and $\text{Flow}_{\text{RCVD}}$ in case of normal traffic/no accident and all HNs.

an accident occurs at $t = 180$ s for the same density of vehicles. Similarly, Figs. 7 and 8 show the results when the density is kept constant and the update interval is varied. It can be seen from Figs. 6–8 that the density has a negligible effect on the working of the method, i.e., all vehicles receive the information about the attack at the same time [i.e., figures in the same column such as Figs. 6(b), 7(b), and 8(b)] if the update interval is the same. This shows that the proposed mechanism is scalable. In addition, it is clear that the update interval has a significant impact on the information flow as the value settles down the quickest in Figs. 6(c), 7(c), and 8(c) when the update interval is the smallest, i.e., 0.2 s, as compared with the others when the update interval is higher. However, this is acceptable as the standard update interval in VANETs can be as low as 100 ms or 0.1 s.

2) Normal Traffic—No Accident—No Rogue Nodes: There is a need to record the traffic data in case of normal traffic, i.e., no accident and no RNs, to see how the system works. Fig. 9 shows the recorded data for the 100th node when the update interval is 1 s and the inter-arrival rate is 1 s. As expected, the average value of flow, i.e., Flow_{AVG}, the calculated values for flow, i.e., Flow_{OWN}, and the received flow values from other vehicles, i.e., $\text{Flow}_{\text{RCVD}}$, are all quite close to each other, and the received values $\text{Flow}_{\text{RCVD}}$ are, in fact, within one standard deviation of Flow_{AVG}, as calculated by the node.

3) No Accident—RNs: A scenario is simulated in which there is no accident but RNs start transmitting a low false value of flow after $t = 160$ s. We run the simulations both with and without the proposed IDS and also vary the number of rogue/malicious nodes and collect the data. The results are shown with and without the proposed IDS in Fig. 10, when there are 20% RNs. As shown in Fig. 10(b), the flow value goes down first while the IDS runs the hypothesis tests to evaluate the received data and then starts to reject the false values. However, in the absence of the IDS (see Fig. 10(a)), the flow value is reduced, as all the values are accepted.

4) Accident Scenario—Rogue Nodes: An accident scenario is simulated where RNs start transmitting false (high) values after $t = 230$ s after an accident has occurred to deny the accident. The simulation is run both with and without the IDS, and the results are shown in Fig. 11(a) and (b), respectively. It can be seen in Fig. 11(b) that the very high values by RNs are being rejected by the IDS.

C. Evaluation Metrics

We test our IDS by computing the true positive (TP) rate (detection rate), the FP rate, and the detection time. The number of RNs was increased from 5% to 40% to test how successfully the proposed IDS classifies RNs as rogue and HNs as honest. We also compare our results with that of two previous schemes that deal with false information attacks, i.e., [15] and [24]. The metrics used are described in the following.

1) True Positive: This is the detection rate of RNs, i.e., what percentage of RNs is detected and classified as RNs. This is also referred to as sensitivity and is calculated as follows:

$$\text{TP} = \frac{\text{Number of RNs detected correctly}}{\text{Total number of RNs}}. \tag{7}$$

2) False Positive: This is the percentage of HNs incorrectly classified as RNs. Specificity is defined as the number of HNs correctly identified and is given as

$$\text{Specificity} = \frac{\text{Number of HNs identified correctly}}{\text{Total number of HNs}} \tag{8}$$

and the FPs are calculated as follows:

$$\text{FP} = 1 - \text{Specificity}. \tag{9}$$

3) Overhead: Overhead is the cost incurred due to the IDS working and the extra data that are exchanged with other vehicles. It is an important metric as it is a measure of the efficiency of any scheme.

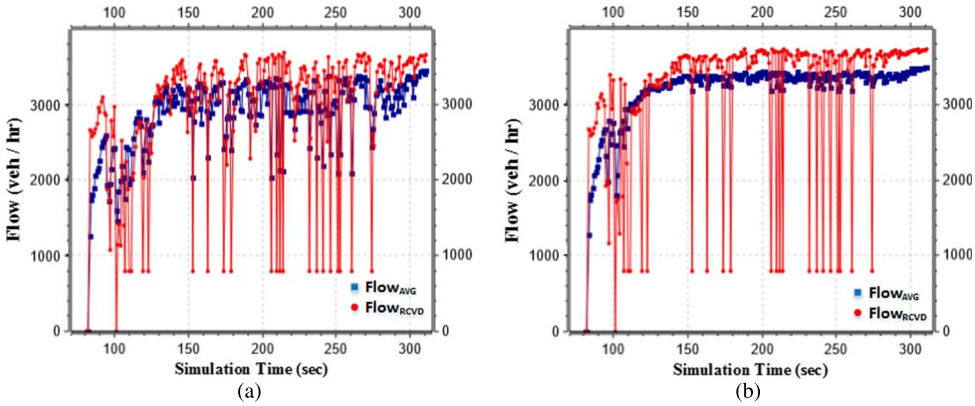

Fig. 10. No-accident scenario: 20% RNs—start transmitting false values at $t = 160$ s. (a) Flow_{AVG} without IDS. (b) Flow_{AVG} with IDS.

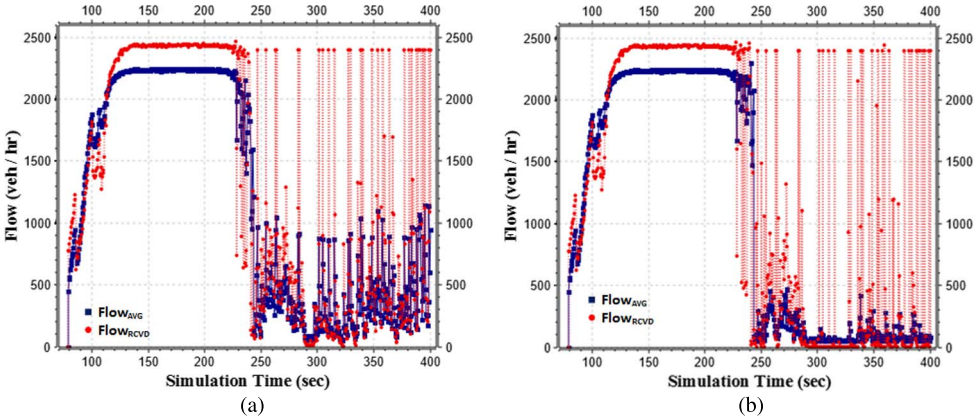

Fig. 11. Accident scenario: 20% RNs—start transmitting false values at $t = 230$ s. (a) Flow_{AVG} without IDS. (b) Flow_{AVG} with IDS.

D. Effectiveness of Hypothesis Testing

The adoption of hypothesis testing works very well to determine whether the received data are correct or not. The t-test works very well to determine whether the data are false or not, thereby concluding if the node is rogue or honest. The t-test compares the population means of two populations and ascertains if the means of the two populations are increasing or decreasing together. The simulation confirms that, when the nodes are honest, then the vehicles that are close together will have very similar flow values (see Fig. 9). This is true in all cases, i.e., both in case of an accident and free-flowing traffic.

The cases simulated in this paper are the worst case scenarios, i.e., coordinated attacks by RNs. This means that all RNs work together and launch the attack at the same time to cause maximum damage. Such a coordinated attack is not only difficult to launch but very expensive as well as it requires rogue vehicles to be placed together in strategic positions.

VI. Discussion

Here, we discuss the performance of the proposed intrusion detection mechanism on the network and its reliability and robustness under changing parameters. We also compare our work with previously proposed approaches.

A. False Information Attack Detection

The proposed IDS is able to detect false information attacks very effectively by only analyzing the data without taking into account any trust or reputation scores. The proposed mechanism is compared with two schemes, i.e., DCMD [15] and ELIDV [24]. The detection rates are shown in Fig. 12(a), and the FP rates are compared in Fig. 12(b). The detection rate (TPs) of the proposed scheme is better than that of DCMD and ELIDV up to 30% RNs and almost the same as that of ELIDV after that until 40%. The FP rate of the proposed scheme is better than that of DCMD and ELIDV up to 20% RNs but increases slightly above ELIDV at 40%.

B. Resilience to Sybil Attacks

In a Sybil attack, an attacker presents multiple identities with an intent to either create the illusion of congestion or accidents or deny their existence. Thus, a rogue vehicle will send multiple messages to cause confusion in the network by bringing the parameter value down. However, the proposed IDS aggregates the parameter values; therefore, the IDS will work very well and will be resilient to Sybil attacks, as long as the total number of Sybil identities is less than 40% of the total identities (nodes), as shown in Fig. 12(a) and (b).

C. Overhead Comparison

The overhead of the proposed IDS is compared with the schemes in [15] and [24], and the results are shown in Fig. 12(c). The overhead in the proposed IDS is less compared with that in DCMD and ELIDV, except when there are 40% nodes, at which point, it is slightly higher than that in DCMD.

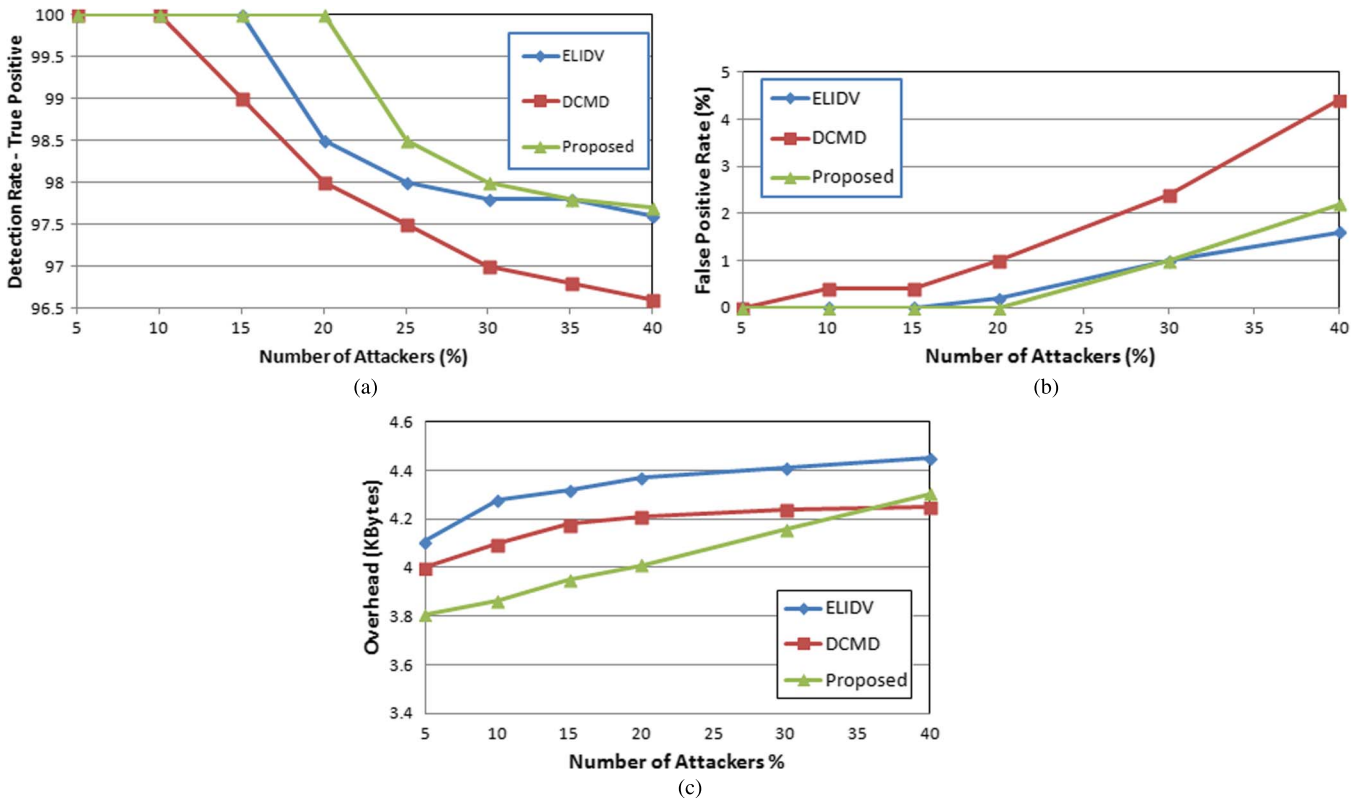

Fig. 12. Comparison of the proposed IDS. (a) Detection rate comparison in case of false information attack. (b) FP rate comparison in case of false information attack. (c) Overhead comparison in case of false information attack.

The overhead in the proposed IDS increases with the increase in the number of RNs as the IDS starts to collect more past values to run the hypothesis test. However, the proposed IDS does not need to keep past parameter values as long as they agree with the calculated values, which is why the initial overhead is low.

D. Quick Response of IDS

The analysis shows that the test can be successfully conducted by taking only seven samples from an RN, i.e., the node that is incorrectly transmitting a false value, and performing the t-test on the population mean of two populations. The seven samples can be collected in a minimum of 0.7 s if the beaconing rate is 100 ms. This means that the IDS enables the nodes to quickly decide whether to accept or reject the data received without generating a lot of overhead.

E. Countermeasures and Fault Tolerance

The proposed VANET model and exchange of parameters give the vehicular network a built-in resilience to launch countermeasures against false information attacks. The data are highlighted as false or malicious if they do not conform to the VANET model or if they fail the hypothesis test. The countermeasures include rejecting the data of that node and reporting the node as malicious. This is shown in Figs. 10(b) and 11(b), where the values were too low or too high compared with the node's own values and were detected (and then rejected) by the IDS. The IDS is therefore fault tolerant, as it can work in the presence of false information.

F. Effective Information Dissemination

The widely proposed method of propagating emergency messages is by repeatedly broadcasting the message by vehicles to others behind them. This can quickly cause a broadcast storm in an already bandwidth-limited channel. In the proposed scheme, there is no channel congestion as there is no need for multihop retransmissions and the information is still disseminated effectively.

G. Limitations of the Proposed IDS

The proposed IDS works extremely well when the difference between the received values and the calculated values is high, i.e., the values being received from the RNs are too high or too low. However, if the RNs coordinate and gradually decrease (or increase) their parameter values and launch the attack over some time, then it will be very difficult to detect the attack. The reason is that the gradual decrease in the parameter values will not be flagged as an anomaly and, thus, never tested for correctness. However, as previously discussed, doing this defeats the main purpose of the rogue/malicious vehicles, i.e., to cause maximum damage or confusion in the network.

VII. Conclusion and Future Work

In this paper, an IDS has been developed and tested, and the results have been discussed. The results show that the proposed IDS is scalable and has an excellent performance when the number of RNs is small. The performance degrades when the number of RNs increases but still works reasonably well. The proposed model and IDS demonstrate the effectiveness

of the statistical technique used to determine if the data are false based on the overall collected data without using trust or reputation scores. The IDS depends on no infrastructure, which is a major benefit as compared with other schemes. The false data are much easier to detect if they differ too greatly from the calculated data and difficult to detect if they vary slightly. However, the target of the RN is to drop or raise the value of its parameters quickly to damage the network, and raising or dropping it gradually is not in its interest.

In the future, the work can be extended by modifying the IDS to detect other types of attacks in VANETs, such as denial of service and false position reporting by RNs in the network or a stationary user outside the network. This can be done by simulating the attacks using the developed platform and then detecting them with the help of anomaly or rule-based detection.

REFERENCES

[1] H. Sedjelmaci and S. M. Senouci, "A new intrusion detection framework for vehicular networks," in *Proc. IEEE ICC*, 2014, pp. 538–543.

[2] H. Sedjelmaci, S. M. Senouci, and M. Feham, "An efficient intrusion detection framework in cluster-based wireless sensor networks," *Security Commun. Netw.*, vol. 6, no. 10, pp. 1211–1224, Oct. 2013.

[3] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in *Proc. 6th Annu. IEEE Commun. Soc. Conf. SECON*, 2009, pp. 1–9.

[4] D. Huang, S. Misra, G. Xue, and M. Verma, "PACP: An efficient pseudonymous authentication based conditional privacy protocol for VANETS," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 736–746, Sep. 2011.

[5] A.-N. Shen, S. Guo, D. Zeng, and G. Mohsen, "A lightweight privacy-preserving protocol using chameleon hashing for secure vehicular communications," in *Proc. IEEE WCNC*, 2012, pp. 2543–2548.

[6] R. Lu, X. Li, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, Jan. 2012.

[7] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security Spec. Issue Security Ad Hoc Sensor Netw.*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[8] P. Papadimitratos, A. Kung, J. P. Hubaux, and F. Kargl, "Privacy and identity management for vehicular communication systems: A position paper," presented at the Workshop Standards Privacy User-Centric Identity Manag., Zurich, Switzerland, Jul. 2006.

[9] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE 27th Conf. Comput. Commun.*, Apr. 2008, pp. 1229–1237.

[10] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communication," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[11] Vehicle Safety Communications Project Final Report: Identify Intelligent Vehicle Safety Applications Enabled by DSRC, U.S. Dept. Transp., Nat. Highway Traffic Safety Admin., Washington, DC, USA, 2005.

[12] K. A. Hafeez, L. Zhao, B. Ma, and J. W. Mark, "Performance analysis and enhancement of the DSRC for VANET's safety applications," *IEEE Trans. Veh. Technol.*, vol. 62, no. 7, pp. 3069–3083, Sep. 2013.

[13] F. Kargl *et al.*, "Secure vehicular communication systems: Implementation, performance, and research challenges," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 110–118, Nov. 2008

[14] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw.*, 2004, pp. 29–37.

[15] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On data-centric misbehavior detection in VANETs," in *Proc. VTC Fall*, 2011, pp. 1–5.

[16] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[17] P. Wex, J. Breuer, A. Held, T. Leinmuller, and L. Delgrossi, "Trust issues for vehicular ad hoc networks," in *Proc. VTC Spring*, May 11–14, 2008, pp. 2800–2804.

[18] L. Qin, A. Malip, K. M. Martin, S. Ng, and J. Zhang, "A reputation-based announcement scheme for VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 9, pp. 4095–4108, Nov. 2012.

[19] U. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expanded trust management for agents in vehicular ad hoc networks," *Int. J. Comput. Intell. Theory Pract.*, vol. 5, no. 1, pp. 3–15, Jun. 2010.

[20] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in *Proc. 3rd Annu. Int. Conf. Mobile Ubiquitous Syst.*, 2006, pp. 1–8.

[21] M. Baguena *et al.*, "VACaMobil: VANET car mobility manager for OMNeT++," in *Proc. IEEE ICC*, Jun. 2013, pp. 1057–1061.

[22] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO—Simulation of urban mobility: An overview," in *Proc. SIMUL*, Oct. 2011, pp. 63–68.

[23] K. Zaidi, M. Milojevic, V. Rakocevic, and M. Rajarajan, "Data-centric rogue node detection in VANETs," in *Proc. IEEE 13th Int. Conf. TrustCom*, 2014, pp. 398–405.

[24] H. Sedjelmaci, S. M. Senouci, and M. A. Abu-Rgheff, "An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks," *IEEE Internet Things J.*, vol. 1, no. 6, pp. 570–577, Dec. 2014.

[25] N. Bimeyer, C. Stresing, and K. M. Bayarou. "Intrusion detection in VANETs through verification of vehicle movement data," in *Proc. IEEE VNC*, 2010, pp. 166–173.

[26] E. M. Shakshuki, N. Kang, and T. R. Sheltami, "AACKA secure intrusion–detection system for MANETs," *IEEE Trans. Ind. Electron.*, vol. 60, no. 3, pp. 1089–1098, Mar. 2013.

[27] J. Hortelano, J. C. Ruiz, and P. Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs," in *Proc. IEEE ICC*, 2010, pp. 1–5.

[28] H. Sedjelmaci, T. Bouali, and S. M. Senouci, "Detection and prevention from misbehaving intruders in vehicular networks," in *Proc. IEEE Globecom*, Austin, TX, USA, Dec. 8–12, 2014, pp. 39–44.

[29] T. Gazdar, A. Rachedi, A. Benslimane, and A. Belghith, "A distributed advanced analytical trust model for VANETs," in *Proc. IEEE Globecom*, Anaheim, CA, USA, 2012, pp. 201–206.

[30] H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," *Comput. Electr. Eng.*, vol. 43, pp. 33–47, Apr. 2015.

Kamran Zaidi received the B.E. degree in electrical engineering from National University of Sciences and Technology, Islamabad, Pakistan, in 1999 and the M.Sc. degree in electronics engineering from London Metropolitan University, London, U.K., in 2003. He is currently working toward the Ph.D. degree in information engineering with City University London.

His research interests include security and privacy of wireless and wired networks, with focus on intrusion detection, cryptography, and identity management.

Milos B. Milojevic (S'13) received the B.Sc. and M.Sc. degrees in electrical engineering from the University of Belgrade, Belgrade, Serbia, in 2009 and 2010, respectively. He is currently working toward the Ph.D. degree in electronic engineering with City University London, London, U.K.

His research interests include vehicular ad hoc networks, intelligent transport systems, data aggregation, and message dissemination in vehicular ad hoc networks.

Veselin Rakocevic (M'01) received the Dipl.Ing. degree in electronic engineering from the University of Belgrade, Serbia, in 1998 and the Ph.D. degree in electronic engineering from Queen Mary University of London, London, U.K., in 2002.

Since 2002, he has been a Reader in electronic engineering with City University London. His main research interest is in the operation of multihop wireless networks, particularly addressing the problems of optimal scheduling, rate control, and quality of service, with applications to vehicular networks and wireless sensor networks.

Arumugam Nallanathan (S'97–M'00–SM'05) received the B.Sc. degree with honors from the University of Peradeniya, Sri-Lanka, in 1991; the CPGS degree from the University of Cambridge, Cambridge, U.K., in 1994; and the Ph.D. degree from the University of Hong Kong, Hong Kong, in 2000, all in electrical engineering.

He is currently a Professor of wireless communications with the Department of Informatics, King's College London, University of London, London, U.K. He served as the Head of Graduate Studies with the School of Natural and Mathematical Sciences, King's College London, from 2011 to 2012. He was an Assistant Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore, from August 2000 to December 2007. His research interests include fifth-generation technologies, millimeter-wave communications, cognitive radio, and relay networks. In these areas, he has coauthored more than 250 papers.

Prof. Nallanathan served as the Chair for the Signal Processing and Communication Electronics Technical Committee of the IEEE Communications Society, Technical Program Co-Chair (MAC Track) for the 2014 IEEE Wireless Communications and Networking Conference, Co-Chair for the 2013 IEEE Global Communications Conference (GLOBECOM; Communications Theory Symposium), Co-Chair for the 2012 IEEE International Conference on Communications (ICC; Signal Processing for Communications Symposium), Co-Chair for IEEE GLOBECOM 2011 (Signal Processing for Communications Symposium), Technical Program Co-Chair for the 2011 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB), Co-Chair for IEEE ICC 2009 (Wireless Communications Symposium), Co-Chair for IEEE GLOBECOM 2008 (Signal Processing for Communications Symposium), and General Track Chair for the 2008 IEEE Vehicular Technology Conference. He is an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and a Guest Editor of the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING Special Issue on Advances in Mobile and Cloud Computing. He was an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS (2006–2011), IEEE WIRELESS COMMUNICATIONS LETTERS, and IEEE SIGNAL PROCESSING LETTERS. He received the IEEE Communications Society SPCE Outstanding Service Award in 2012 and the IEEE Communications Society RCC Outstanding Service Award in 2014. He coreceived the Best Paper Award at IEEE ICUWB in 2007. He is a Distinguished Lecturer of the IEEE Vehicular Technology Society.

Muttukrishnan Rajarajan (SM'05) received the B.Eng. degree in electrical and electronics engineering and the Ph.D. degree in information engineering in 1995 and 1999, respectively, from City University London, London, U.K.

He is a Full Professor of security engineering with City University London, where he leads the Information Security Group. He has actively participated in several cyber-security debates in the U.K., Europe, and internationally and continues to act as an Advisor to the Government of India cyber-security laboratories in the area of supervisory control and data acquisition security and identity management. He also advises the U.K. Government's identity assurance program in the areas of access control and privacy. His research interests are in the areas of identity, privacy, and intrusion detection. He has published more than 200 papers in these areas.

Prof. Rajarajan is an Advisory Member of the Institute of Information Security Professionals, U.K. He continues to be involved with the Editorial Boards and Technical Program Committees of several international conferences and journals. He was chosen as one of the leading academics with outstanding research impact in the security community.