Multi-BSM: An Anomaly Detection and Position Falsification Attack Mitigation Approach in Connected Vehicles

Zouheir Trabelsi
United Arab Emirates University

Syed Sarmad Shah
School of Electrical Engineering and Computer Science

Kadhim Hayawi
Zayed University

Recommended Citation

Trabelsi, Zouheir; Shah, Syed Sarmad; and Hayawi, Kadhim, "Multi-BSM: An Anomaly Detection and Position Falsification Attack Mitigation Approach in Connected Vehicles" (2022). *All Works*. 5459.
https://zuscholars.zu.ac.ae/works/5459

electronics

MDPI

Article

Multi-BSM: An Anomaly Detection and Position Falsification Attack Mitigation Approach in Connected Vehicles

Zouheir Trabelsi [1,*], Syed Sarmad Shah [2] and Kadhim Hayawi [3]

[1] College of Information Technology, United Arab Emirates University (UAEU), Al-Ain P.O. Box 15551, United Arab Emirates
[2] School of Electrical Engineering and Computer Science, National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan
[3] College of Technological Innovation, Zayed University, Dubai P.O. Box 144534, United Arab Emirates
[*] Correspondence: trabelsi@uaeu.ac.ae

Abstract: With the dawn of the emerging technologies in the field of vehicular environment, connected vehicles are advancing at a rapid speed. The advancement of such technologies helps people daily, whether it is to reach from one place to another, avoid traffic, or prevent any hazardous incident from occurring. Safety is one of the main concerns regarding the vehicular environment when it comes to developing applications for connected vehicles. Connected vehicles depend on messages known as basic safety messages (BSMs) that are repeatedly broadcast in their communication range in order to obtain information regarding their surroundings. Different kinds of attacks can be initiated by a vehicle in the network with malicious intent by inserting false information in these messages, e.g., speed, direction, and position. This paper focuses on the position falsification attacks that can be carried out in the vehicular environment and be avoided using the multi-BSM approach. Multi-BSM uses consecutive multiple BSMs with different parameters to detect and warn other vehicles about position falsification attacks. Multi-BSM is compared to other anomaly detection algorithms and evaluated with rigorous simulations. Multi-BSM shows a high level of anomaly detection, even in high vehicle density, with up to 97% accuracy rate compared to the respective algorithms.

Keywords: connected vehicles; safety; BSM; anomaly detection

Citation: Trabelsi, Z.; Shah, S.S.; Hayawi, K. Multi-BSM: An Anomaly Detection and Position Falsification Attack Mitigation Approach in Connected Vehicles. *Electronics* **2022**, *11*, 3282. https://doi.org/10.3390/electronics11203282

Academic Editors: Flavio Canavero and Juan-Carlos Cano

Received: 21 August 2022
Accepted: 10 October 2022
Published: 12 October 2022

1. Introduction

Connected vehicles are the face of transportation systems. Through these, the transportation system is upgraded to an intelligent transportation system. The quality of the daily commute is being improved, and the communication is getting better. Safety applications are being developed for the betterment of the vehicular environment. Vehicular networks are being upgraded for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, which directly affects the wellbeing of the daily commuters. The road side units (RSUs) play a vital role for the connected vehicles in the V2I communications. These technologies empower dynamic communication in real time for the vehicular environment. Nowadays, security and privacy are the most sought-after aspects regarding networks. In [1], the authors comprehensively surveyed the authentication and privacy schemes related to vehicular ad hoc networks (VANETs).

A lot of data are shared through the vehicular network and are made available for the consumption of the surrounding vehicles. This information contains important events as well as regular updates about the generating source. Important events can be classified as data regarding any road accidents, heavy traffic, and/or any relevant urgent information that needs to be addressed in real time, whereas regular updates are messages that are periodically generated by vehicles informing others about their speed, location, heading, etc., known as basic safety messages (BSMs). In an ideal situation, the information is disseminated flawlessly in connected vehicles, but in actuality, this information is vulnerable to attacks initiated by malicious attacker vehicles present in the network. Schemes need to be adopted to counter and detect attacks that are currently exploiting the network. In [2], the authors surveyed identity-based cryptographic schemes used for the security and privacy concerns in VANETs. The protection and safeguarding of the regular updates are as vital as the important messages that are disseminated in a timely manner, as any potential attacker could be listening in on the regular updates of the connected vehicles and could launch different types of attacks depending on the attacker's intention. In [3], the authors proposed a secure data-sharing scheme for 5G-enabled vehicular networks without using the RSUs.

Preventive measures need to be implemented to avoid any misfortunes. These attacks could harm individuals either directly or indirectly. The attacks could be active in nature, in which the attacker modifies the contents of the messages being disseminated, or the attack could be passive, in which the attacker just listens to the information being conveyed from one end to the other and uses it for its personal gains. Mechanisms are needed to check for anomalies in the behavior of the connected vehicles present in the network to detect whether they are legitimate vehicles or malicious attackers with ill intent. Such disturbances cause harm to the commuters and degrade the performance of the network, and they need to be dealt with swiftly. In [4], the authors proposed a privacy-preserving authentication scheme known as CM-CPPA in 5G-enabled vehicular networks while decreasing the overhead of communication.

The vehicular network is exposed to different kinds of attacks, and if preventive measures are not taken then they could harm the individuals directly or indirectly. One such attack is a black hole attack [5], in which the malicious nodes place themselves in a suitable position in the network where the effects of the attacks can be maximized. The malicious nodes pretend to have an optimal route for the dissemination of messages in order to lure more vehicles. When the messages are sent to these malicious nodes, they either drop the messages, redirect them, or use them for their own nefarious purposes. Another attack that is orchestrated by the malicious nodes in the vehicular network is that of a Sybil attack [6]. In this attack, the malicious node initiates the illusion of the existence of multiple vehicles in the network and generates false information in order to take control of the available network. The purpose of this attack could be to cause detriment of the performance of the network or to harm the legitimate vehicles themselves. Another form of attack that proves dangerous in the network is that of a wormhole attack [7]. This is somewhat similar to the black hole attack, in which at least two malicious attacker nodes place themselves in an optimum position to enhance the damage of their attack and form a tunnel with the lowest number of hop counts to entrap other legitimate vehicles for opting for the attacker's tunnel route. Once the legitimate vehicles start sending messages through the attacker's route, the malicious nodes can do anything with the received information; they can either drop the message, modify it, redirect it, or eavesdrop on it. Position falsification attack [8] is another critical attack that can be deployed in connected vehicles. In this attack, the malicious attacker broadcasts false information regarding the position of the vehicles through safety messages that are generated on a periodic basis. This attack can create confusion among the connected vehicles and can cause severe repercussions.

Safety applications are being deployed in the vehicular network to achieve the required safety and convenience for individuals. For these applications to work optimally and stay up to date, connected vehicles need to be made aware of their surrounding environment through BSMs. Through these messages, the connected vehicles are updated about their surroundings and make appropriate decisions regarding any event. The BSMs need to be generated and transmitted in real time because they become irrelevant after a certain period of time, e.g., the information about a vehicle's speed and location may be useless after an hour or two later unless it is used by law enforcement authorities. Due to the time-criticality, these messages are often not encrypted. Some mechanisms may encrypt BSM as well, but at the cost of the network performance [9]. These BSMs are exposed to various attacks that can be initiated in the network which can cause severe harm to the victims. Figure 1 shows a scenario in which the RSU detects an attacker vehicle and relays information to other RSUs and vehicles.

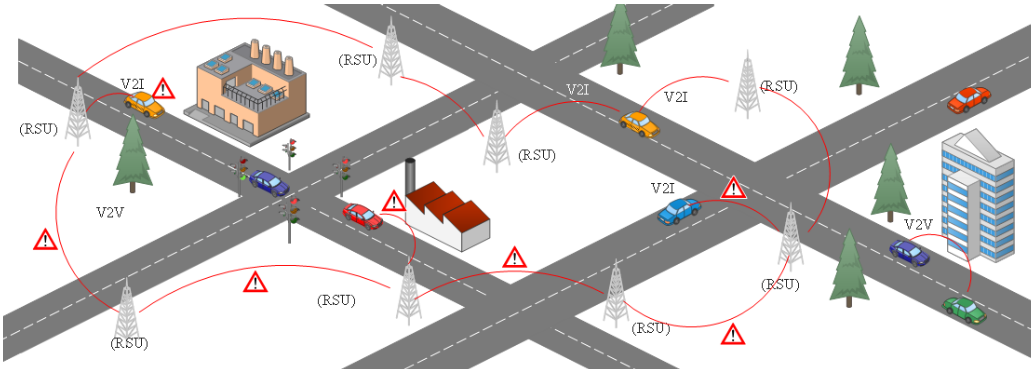


Figure 1. RSU detecting an attacker and forwarding information to other connected RSUs and vehicles.

Our proposed scheme uses the multi-BSM approach for anomaly detection; more specifically, position falsification attacks. The proposed scheme compares multiple consecutive BSMs from the same vehicles based on multiple parameters, i.e., location, speed, and direction. It is assumed that all RSUs are linked with each other and are connected with a central database. It is also assumed that Global Positioning System (GPS) systems of genuine vehicles are working correctly. Only malicious vehicles tamper with the GPS data. Our work targets the detection and prevention of position falsification attacks in a connected vehicular environment. The salient features of the papers are following:

- The detection of position falsification attacks using multiple consecutive BSMs utilizing parameters such as position, speed, and direction is proposed.
- The RSUs are used for the detection of position falsification attacks, as onboard units (OBUs) of the vehicles have limited resources and may not be connected to the central database in real time.
- Preventing vehicles from falling victims to the attacks of a malicious node even before entering the transmission range of the attacker with the help of RSUs.

Section 2 reviews the work that has been accomplished in the connected vehicles regarding anomaly detection and security attacks. The preliminaries and the system model are discussed in Section 3. The proposed scheme is elaborated in Section 4. After that, performance evaluation is discussed in Section 5, followed by conclusion and future work in Sections 6 and 7. Lastly, acknowledgments are addressed.

2. Literature Review

The connected vehicles are susceptible to different types of attacks in the vehicular environment. An effective mechanism is needed to detect and prevent these attacks to ensure the safety of the individuals. The work that has been carried out in this regard is discussed in this section. Table 1 lists some of the network attacks and the detection algorithms used for the respective attacks.

Meyer et al. [10] worked on the detection of network anomalies, e.g., DDoS, by implementing their proposed scheme on the link layer. They also worked on the deployment of an SDN controller for reconfiguring the network when an attack is being carried out or in the case of an incident, conveying the information to a cloud infrastructure. It has been seen that connected vehicles are vulnerable to many attacks when it comes to a realistic vehicular environment by exploiting messages that are injected into the controller area network (CAN) bus. In [11], Othmane et al. proposed a mechanism that could detect whether the vehicle is under attack or not by using the revolutions per minute (RPM) and speed reading. They used the k-means clustering method and HMM to characterize the vehicles as either under attack or no attack. They had acceptable detection and accuracy rate but also a high false-positive rate.

In today's era, 5G helps in improving the data transmission between vehicles in a connected environment, but with the increase in the exchange of information, there is also a rise in the attacks on the network. Ji et al. [12] explored the conceivable attacks that could be initiated in a vehicular network regarding 5G and came up with intrusion detection mechanisms to counter such attacks by comparative study. Grover et al. [13] used an algorithm that detects anomalies in BSMs by monitoring the inconsistencies in position and speed with which the vehicles generate packets. The detection algorithm runs at RSUs.

The investigation of in-vehicle communication is a gap that needs to be filled with extensive research, and researchers are improving daily to detect and prevent the network attacks that are carried out in the connected vehicles. Stabili et al. [14] proposed a mechanism for intrusion detection whose main goal is to recognize the hostile messages that are targeted at the CAN bus. The proposed algorithm was developed and administered with low-end electronic control units (ECUs).

Table 1. Comparison of different attacks and proposed algorithms in connected vehicles.

	Suitable Area	Information Coverage	Attack Type	Detection Algorithm	Simulator
Katragadda et al. [15]	Generic	✓	Replay-based injection	Subsequence mining	-
Comert et al. [16]	Generic	✓	DOS, impersonation	EM, CUSUM	-
Negi et al. [17]	Generic	✓	Misbehaviour	LSTM	MXNet
Petrenkov et al. [18]	Generic	✓	Spoofing	Consensus control	Plexe, OMNeT++
D'Angelo et al. [19]	Generic	✓	DOS, fuzzy, RPM	Cluster-based, data-driven	MATLAB
Berlin et al. [20]	Generic	✓	Credentials theft	SeMaCoCa	-
Gautham et al. [21]	Generic	✓	Black hole	AODV	NS2
Leinmuller et al. [22]	Urban/motorway	✓	Position falsification	Cooperative position verification	NS2
Heijden et al. [23]	Urban	✓	Position falsification	Subjective logic	OMNeT++, SUMO, VEINS
Grover et al. [13]	Highway	✓	Position falsification	RSU verification	NCTUns
Boeira et al. [24]	Highway	✓	Position falsification	Vouch	Plexe, OMNeT++
Proposed scheme	Urban	✓	Position Falsification	Multi-BSM	OMNeT++, SUMO, VEINS

Connected vehicles play a vital role in the uprising of the intelligent transportation system, and the connectivity is increasing on a daily basis. Such connectivity does not require elaborate attacks to disturb the flow of the traffic, just some misleading data would be enough for the job. Ranaweera et al. [25] proposed traffic flow theory to improve the detection of anomalous data which can lead to attacks in the vehicular environment. Their results displayed uniform and reliable foresight, while in Boeira et al. [24], the 5G-enabled wireless RSUs employ the proof-of-location technique, which in turn utilizes the node-positioning capabilities of the RSUs.

The safety of the vehicles in a connected environment is ensured by the continuous exchange of information between the vehicles themselves and the RSUs. Thus, the exchange of information needs to be clear and free of misleading data. A filtering scheme is required to block out fake and misleading information to ensure the safety of individuals in the vehicular network. Xiong et al. [26] proposed a filtering scheme (EDFS) that is established on detection and clustering-based algorithm to detect counterfeit information which relies on the characteristics of the data and context without the help of RSUs.

The availability of the network is one of the crucial factors in the vehicular environment. If the network is not available, then no exchange of information takes place, which can lead to many disastrous events. Haydari et al. [27] focused on the DDoS attacks that targeted the RSUs in the network. A DDoS attack can render a system useless and deprive other entities of its resources. The authors proposed a framework for dealing with the detection and alleviation of low-rate DDoS attacks aimed at the RSUs which are hard to differentiate due to the fact that they evade certain filtering mechanisms.

Due to the highly dynamic and rapid nature of the vehicular network, it has multiple vulnerabilities and is prone to many security attacks, e.g., DoS/DDoS attacks. A security mechanism was proposed by Valentini et al. [28], which prioritizes the wellbeing of individuals in vehicular networks by developing a statistical model which searches for extreme values that can be caused by the DoS/DDoS attacks. The proposed mechanism consumes a considerable amount of MAC frames, ARP requests, and features of DoS/DDoS attacks that are initiated by attacker vehicles with malicious intent.

VANETs always play a crucial role in the development of a new breed of self-driving and semi-self-driving vehicles. Safety and comfort are not only provided to the passengers and drivers, but to the vehicles themselves, though such a network of vehicles is vulnerable to attacks such as black hole, gray hole, and rushing attacks. Alheeti et al. [29] proposed an intelligent intrusion detection system (IDS) that protects the vehicles in the network from the gray hole and rushing attacks by detecting the anomalous behavior of the malicious nodes. These types of attacks are aimed to avert the transmissions that take place between the vehicles and the RSUs which can have fatal consequences for the new breed of self-driving and semi-self-driving vehicles.

An effective misbehavior detection system (MDS) is needed to detect the erroneous information that is transmitted from the insider attacker nodes in the vehicular network. Sultana et al. [30] proposed a software-defined networking (SDN)-based detection framework for misbehaving vehicles with malicious intents. The authors exploited the characteristics of SDN, allowing them to dynamically change the parameters for the input according to the changing network.

Gu et al. [31] proposed a clustering-based detection mechanism for false downstream data in a fog-enabled vehicular environment. The authors used the fog servers to detect the malicious cluster head nodes and their anomalous data. They developed a clustering technique to accurately choose cluster head nodes and edge monitoring nodes for the detection of misbehaving vehicles and their malicious data.

Ensuring trust levels in the vehicular environment is a very important factor that is often neglected. Higher trust levels mean that vehicles can safely exchange information with each other without any worries. A higher trust level also deals with many vulnerabilities that vehicles are exposed to in a connected environment. Li et al. [32] proposed a trust management mechanism that actively detects malicious nodes in the network and prevents their attacks which can degrade or cripple the network, while the use of blockchain ensures the trustworthiness of the data being exchanged.

3. Preliminaries

The multi-BSM is used to detect anomalies in the communication of the connected vehicles, i.e., position falsification attacks, to be more specific. The anomaly detection algorithm runs on the RSUs which are better equipped with more computational resources. It is assumed that all RSUs are connected with each other and the RSUs have real-time communication with a centralized database that contains information about the flagged vehicles and all other relevant information. Multi-BSM is better suited for an urban environment as it is more developed compared to rural areas.

System Model

The channel fading affects the overall network performance, so to model this scenario for wireless communication, the Nakagami distribution [33] is used to represent it.

$$p(x; m, \Omega) = 1 - \frac{\Gamma_{mx^2/\Omega}(m)}{\Gamma(m)} \tag{1}$$

$$= e^{-\frac{m}{\Omega}x^2} \frac{2m^m}{\Gamma(m)\Omega^m} x^{2m-1} \tag{2}$$

The cumulative distributive function for signal reception is represented by $\frac{\Gamma_{mx^2/\Omega}(m)}{\Gamma(m)}$, where x^2 stands for the reception threshold of signal propagation and Γ stands for gamma function. The average power level for the received signal is given as Ω. The fading parameter m is determined on the basis of the distance between the vehicles i and j:

$$m = \begin{cases} 3.0 & : d < 50 \text{ m} \\ 1.5 & : 50 \text{ m} \leq d < 150 \text{ m} \\ 1.0 & : \text{otherwise} \end{cases} \tag{3}$$

The average communication transmission scope [34] of the transmitter can be communicated as

$$\bar{r} = \left(\frac{p_t K}{m \Upsilon_0 W}\right)^{\frac{1}{\beta}} \left(\frac{1}{\beta}\right) \sum_{k=0}^{m-1} \frac{\Gamma\left(1 + \frac{1}{\beta}\right)}{k!} \tag{4}$$

where the transmission power is denoted by p_t, path loss coefficient by β, and the fading coefficient of the Nakagami channel is represented by m. The carrier-to-noise ratio threshold is represented by Υ_0 and the total input noise power of an authentic receiver is indicated by W, whereas K represents the constant for the path loss model and is defined as

$$K = \frac{A_t A_r C^2}{4\pi f_c} \tag{5}$$

The gain of the transmitting antenna is represented by A_t, whereas the gain of the receiving antenna is represented by A_r. The speed of light is denoted by C, and the carrier frequency is expressed as f_c.

The vehicles communicate with each other as well as with neighboring RSUs. Therefore, the time the messages take to propagate from the sending entity to the receiving entity can be calculated as follows [35]:

$$t_p = t_r - t_s \tag{6}$$

The propagation time of the message is represented by t_p; t_r represents the timestamp of the message reception, whereas t_s represents the timestamp of the message of when it was sent.

Using Equation (6) and the average velocity of a vehicle v, the distance between the two entities can be derived as

$$d = t_p \times v \tag{7}$$

If $d > \bar{r}$, then the RSU can forward the relevant important information to the neighboring RSU depending on the direction of the flagged or authentic vehicle.

4. Proposed Scheme (Multi-BSM Approach)

RSUs are responsible for detecting anomalies in the network. It is assumed that all the RSUs are legitimate and no malicious RSU is present. All the RSUs are connected to each other and linked with a centralized database that contains all the relevant important information. The centralized database is only accessed through RSUs and contains information about the connected vehicles present in the network, and the information is available to RSUs in real time.

The multi-BSM approach is used to detect anomalies, i.e., position falsification attacks, to be specific, in the vehicular connected environment. Every vehicle that joins the network shares its basic information such as speed, direction, location, etc., to its surrounding neighbors, e.g., RSUs and other vehicles.

4.1. Attacker's Model

The nature of any attacker in the network can be broken down into the following modes:

4.1.1. Active or Passive Attack

The mode of attack in which an attacker is directly involved in the participation of tempering of the information and/or degrading the network is known as the active attack, while the passive attacker only eavesdrops on the information that is being conveyed in the network which can be used for personal or malicious purposes.

4.1.2. Inside or Outside Attack

The attack in which the individual has valid credentials of the network while initiating the said attack is known as an inside attack, while in the outside attack, the individual does not have authentication.

4.1.3. Malicious or Rational Attack

An attack on the network that is initiated by an individual with the sole aim of personal gains is known as a rational attack, while the aim of the malicious attacker is to harm and degrade the network.

For the simulation purpose, we focused on an active inside attacker whose intention may be rational or malicious. The types of position falsification attacks that were addressed during the simulations are discussed as follows:

- **Attack Type 1:** In this type of position falsification attack, the attacker broadcasts a fixed position in the BSMs that is periodically generated.
- **Attack Type 2:** In this, the attacker broadcasts a random position in the BSMs that is periodically generated.
- **Attack Type 3:** In this, the attacker pretends to be a legitimate vehicle for a certain period by broadcasting genuine information in BSMs and initiates a position falsification attack by broadcasting the same position persistently after a while.

4.2. Detection and Prevention of Position Falsification Attack

As the RSUs are aware of their surroundings and are capable of detecting anomalies in the network when a BSM is received at RSU from a vehicle, it firstly checks all the relevant data in the BSM and scans the centralized database for the previous BSM of the same vehicle. If the previous BSM of the same vehicle does not exist in the records, then the received BSM is documented for that specific vehicle. If the previous BSMs of the same vehicle are found in the records, then the RSU compares the current BSM with the previous BSMs to detect any anomaly that may be present in the concerned data, e.g., position falsification attack that may be initiated by a malicious attacker with an intent to cause harm. These position falsification attack data vary a lot from the legitimate data that are being generated by an authentic vehicle, as the specific fields in the BSM have quite extreme changing of values.Upon the detection of the position falsification attack, the next step is to alert the connected vehicles and prevent any harm that can be caused by such attacks. Algorithm 1 describes the anomaly detection that takes place at an RSU.

Algorithm 1 Anomaly detection at RSU.

```
RSU $\leftarrow M_b$
for $i = 1;\ i{+}{+};\ i < db.size$ do
    if $db.M_b == M_b$ then
        $M_b^t \leftarrow \phi$
        if $M_b == \phi$ then
            flag $M_i$
            broadcast($M_i$)
            transmit($M_i$) $\rightarrow RSU_{M_i^d}$
        else
            $M_b^t = M_b$
        end if
    else
        $db = M_b$
    end if
end for
```

To accurately detect the position falsification attack, the BSMs are thoroughly checked with the previous BSMs of the same vehicle. In order to detect Attack Type 1, the parameters for the location, speed, and direction are analyzed, in which the malicious vehicle is periodically generating the same position. It can be observed that the position of the vehicle is not changing; it is pretending to be at a stationary location, but the values of the speed parameter are not zero, and the direction is also sometimes changing. This triggers the detection of the anomaly present in the BSMs, and the concerned vehicle is flagged as malicious.

In Attack Type 2, the malicious vehicle randomly broadcasts its position through the periodic generation of BSMs, and the RSU, after acquiring these BSMs, analyzes the data. In the respective BSMs, the values for location updates vary a lot from the previously generated location as they are random in nature. These large variations in the location updates trigger the anomaly detection, and the RSU flags the vehicle as malicious because such distances cannot be covered with the given speed of the respective vehicle.

Attack Type 3 is more difficult to detect because the malicious vehicle generates genuine information for some time, containing legitimate information updates on the respective vehicle, but after a while, the malicious vehicle starts broadcasting the same location updates in the BSMs to pretend that the vehicle has come to a stop. The RSU, after accumulating enough BSMs for the respective vehicle, can detect the anomaly in the information by comparing the consecutive BSMs and analyzing the different parameters in the BSM.

After detecting the position falsification attack, the next step is to prevent it. When an RSU detects a malicious attacker, first of all, it flags the vehicle, updates the database, and broadcasts the information about the attacker in its transmission range. The RSU also transmits and alerts other RSUs as they are all connected. The RSU that detected the position falsification attack initiated by the malicious vehicle transmits the relevant information to the other RSUs in the direction of the attacker to prevent the legitimate vehicle from falling victim to the attacker's plan. The Figure 2 shows how a legitimate vehicle B is alerted and made aware of a malicious attacker vehicle A about the position falsification attack even before the legitimate vehicle B came into the transmission range of the attacker vehicle A due to the connectivity of the RSUs between each other. The legitimate vehicles, upon receiving the message about the attacker, store the information on the local log of flagged vehicles. As shown in Figure 2, the first step is detecting a malicious attacker vehicle by RSU. After detection, the RSU, in the next step, transmits the information regarding the malicious attacker vehicle to the neighboring RSU in the direction of the said vehicle. In the next step, the neighboring RSU, upon receiving the information, broadcasts the message to the vehicles in its vicinity. Thus, vehicle B is alerted about vehicle A even before coming into the transmission range of vehicle A. Figure 3 shows the structure of the BSM whereas Figure 4 describes the flow of information at an RSU.

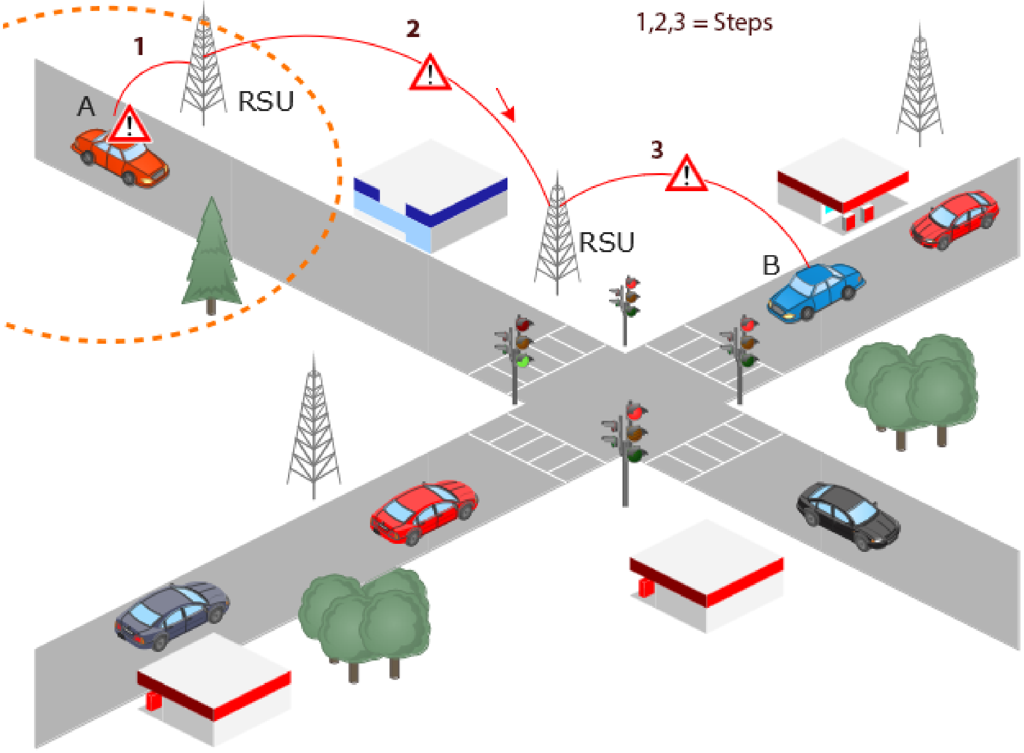
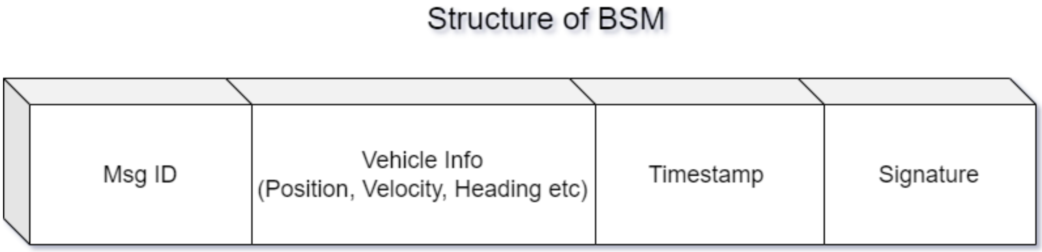


Figure 2. RSU detecting an attacker vehicle and alerting others.



Msg ID	Vehicle Info (Position, Velocity, Heading etc)	Timestamp	Signature

Figure 3. Showing the structure of a basic safety message.

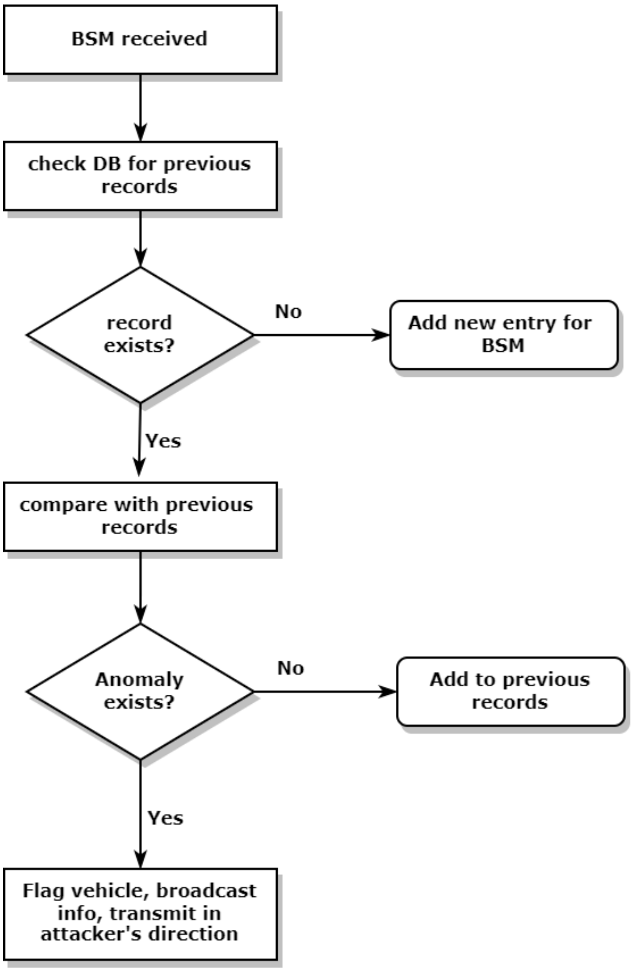

BSM received
check DB for previous records
record exists?
No
Add new entry for BSM
Yes
compare with previous records
Anomaly exists?
No
Add to previous records
Yes
Flag vehicle, broadcast info, transmit in attacker's direction

Figure 4. Multi-BSM.

5. Performance Evaluation

False BSM information can lead to many mishaps, including damage to the vehicles and/or the individuals involved in the said scenario. Misinformation can be very dangerous if not dealt with promptly. The network simulator used to assess the proposed mechanism is OMNeT++ version 5.1.1 [36], together with SUMO version 0.25 [37] and VEINS version 4.6 [38]. The multi-BSM is compared with Grover et al. [13] and vouch scheme [24]. In Grover et al., the algorithm to detect the anomalies in the periodic beacons is operated at the RSUs. According to the algorithm, a vehicle is considered malicious if there are inconsistencies in the position and speed of the generated consecutive packets from the respective vehicle, whereas in the vouch scheme, the proof-of-location method utilizes the node-positioning capabilities of 5G-enabled wireless RSUs.

5.1. Simulation Setup

The simulations are evaluated in an urban scenario. The vehicle density is kept between 30–125 vehicles and inserted at random intervals to simulate the urban environment. The simulations are evaluated for a period of 500 s and an average of 40 runs. Further details about the simulation environment are shown in Table 2.

Table 2. Simulation Parameters.

Parameters	Values
Simulation area	3 km × 3 km
Simulation time	500 s
Simulation runs	40
Transmission range	250 m
Transmission power	20 mW
Road type	Two-way traffic
Data transmission rate	6 Mbps
MAC protocol	IEEE 802.11p WAVE
Vehicle density	30–125/km
Vehicle velocity	12–20 m/s
Maximum acceleration	2.6 m/s^2
Distribution model	Nakagami
EM packet size	170 bytes
Beacon packet size	194 bytes
Road side units	Yes

5.2. Results and Discussion

The proposed and comparison mechanisms are evaluated based on position falsification attacks discussed in the above section, and the accuracy of each anomaly detection mechanism is compared.

The metrics used to evaluate the detection algorithm are described in the following nomenclature.

- **True positive (TP):** The BSM that contains fake or manipulated information regarding the respective vehicle and is correctly identified as an anomaly.
- **True negative (TN):** The BSM that contains legitimate information regarding the respective vehicle and is classified as genuine information.
- **False positive (FP):** The BSM that contains legitimate information regarding the respective vehicle and is incorrectly classified as an anomaly.
- **False negative (FN):** The BSM that contains fake or manipulated information regarding the respective vehicle and is incorrectly identified as genuine information.

The accuracy rate (ACR) is calculated based on the above-given variables as follows:

$$\text{ACR} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{8}$$

Table 3 shows a brief overview of the dataset used for anomaly detection. The parameters **loc_1x**, **loc_1y**, **loc_2x**, **loc_2y**, **loc_3x**, and **loc_3y** are the location coordinates of three consecutive BSMs of each vehicle, whereas **speed_1**, **speed_2**, and **speed_3** are the values of speed in m/sec for the concerned BSMs. The **dir_1**, **dir_2**, and **dir_3** represent the direction of the vehicle in radians for the consecutive BSMs. The **flag** parameters show the status of vehicles, where 0 represents a legitimate vehicle and 1 represents a malicious vehicle.

Table 3. Brief overview of the dataset used for anomaly detection.

Veh No.	loc_1x	loc_1y	speed_1	dir_1	loc_2x	loc_2y	speed_2	dir_2	loc_3x	loc_3y	speed_3	dir_3	Flag
1	1253.61	2271.19	12.12	1.5707	1254.83	2273.54	12.14	1.5713	1255.11	2275.11	12.13	1.5710	0
2	3719.27	6241.43	14.07	0.7142	3721.01	6243.50	14.08	0.7148	3723.89	6244.77	14.08	0.7146	0
3	2593.32	3374.28	15.10	2.7981	2815.32	3624.28	15.11	2.7990	2947.27	3871.82	15.11	2.7985	1
4	1129.07	2316.19	13.76	2.4639	1130.87	2317.38	13.77	2.4677	1132.02	2318.05	13.77	2.4613	0

5.2.1. Impact of Vehicle Density

The density of vehicles always plays a vital role in the evaluation of any proposed algorithm in a connected vehicular environment. As more and more vehicles are connected to the network, the vehicle density can either increase the performance of a certain algorithm with its increase or decrease the performance with increasing density. The algorithms are evaluated with three different densities of vehicles, i.e., low, medium, and high. The low density consists of 30–50 vehicles/km, the medium density consists of 51–80 vehicles/km and the high density consists of 81–125 vehicles/km.

All three algorithms were evaluated in the respective attack scenarios, and each algorithm performed very well when the density of the connected vehicles was kept low, as shown in Table 4. They showed even better performance in Attack Type 3, which is a little harder to detect as compared to the first two attack types.

Table 4. Comparison of accuracy rate in low vehicle density.

Algorithm	Attack Type 1	Attack Type 2	Attack Type 3
Grover et al. [13]	100	100	100
Vouch [24]	100	100	100
Multi-BSM	100	100	100

The respective algorithms were evaluated in the medium vehicle density to inspect the accuracy rate of each algorithm, as shown in Table 5. It was observed that the algorithms performed well when it came to the first two attack scenarios; however, there was a slight decrease in the accuracy rate regarding the Attack Type 3 scenario as the attacker vehicle pretended to be a legitimate vehicle for some time before initiating the position falsification attack.

Lastly, the accuracy rate of the algorithms was evaluated in the high density of connected vehicles ranging from 81–125 vehicles/km as shown in Table 6. The first two attack scenarios were accurately detected by multi-BSM and vouch scheme; however, Grover et al. showed a little decrease in the accuracy rate of Attack Type 2. All the three compared algorithms showed a decrease in accuracy rate regarding Attack Type 3, with Grover et al. being the lowest in comparison to the other two algorithms.

Table 5. Comparison of accuracy rate in medium vehicle density.

Algorithm	Attack Type 1	Attack Type 2	Attack Type 3
Grover et al. [13]	100	99	97.1
Vouch [24]	100	100	98.2
Multi-BSM	100	100	99

Table 6. Comparison of accuracy rate in high vehicle density.

Algorithm	Attack Type 1	Attack Type 2	Attack Type 3
Grover et al. [13]	100	98	94.9
Vouch [24]	100	100	96.3
Multi-BSM	100	100	97

Figure 5 shows the correlation between energy consumption and vehicle density in the increasing order at the RSU. It can be seen that the vouch algorithm consumes the most energy as the density of the vehicles is increased. The multi-BSM and Grover algorithms are somewhat similar in consumption of the energy, with the multi-BSM being a bit higher.

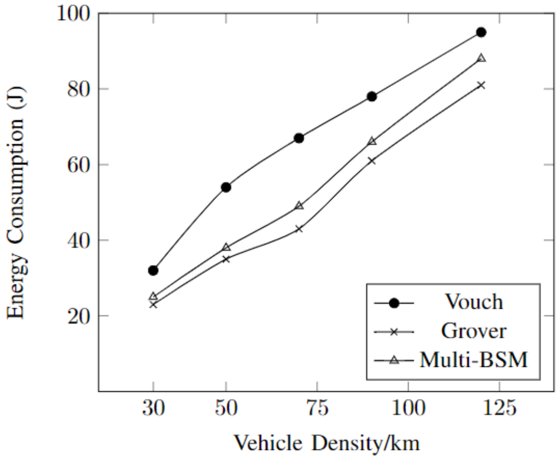


Figure 5. The energy consumption of the algorithms at the RSU.

5.2.2. Impact of Different Intervals on BSM

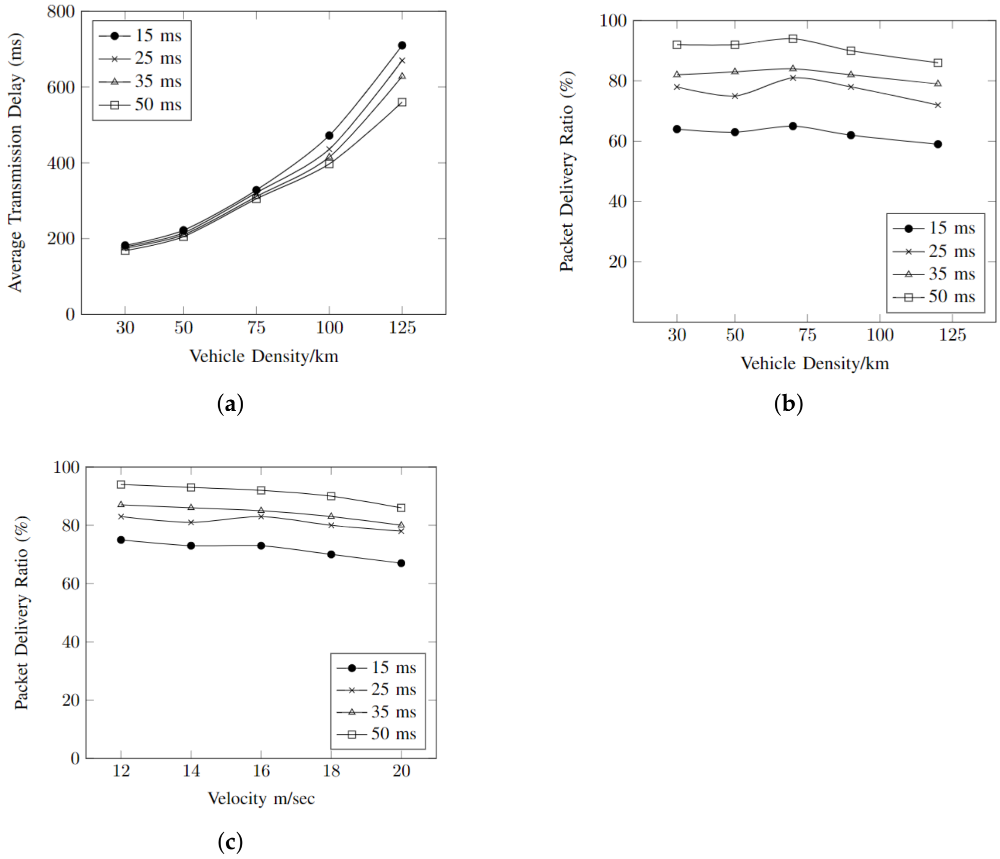
The different intervals with which the BSMs are generated also affect the performance of the multi-BSM. As more vehicles enter the connected environment, more BSMs are generated, and if the generation interval is kept very low then it could clutter the network performance. The control messages also need to be regulated so that they do not clog the network for other emergency messages that need to be disseminated in a timely manner. Therefore, the intervals of BSMs generation also play a vital role in the performance of the multi-BSM.

Figure 6a shows the relationship between the increasing vehicle density with average transmission delay regarding the different intervals. It can be seen that the average transmission delay is kept at the lowest with the increase in the vehicle density when the generation interval is kept at 50 ms.

Figure 6b shows the relationship between the packet delivery ratio with increasing vehicle density regarding different intervals. As more vehicles are entering the network, more BSMs are being generated, which in turn affects the packet delivery ratio; therefore, a suitable interval should be adoptedto improve the packet delivery ratio. As seen in Figure 6b, the packet delivery ratio is at its lowest when the BSM interval is kept at 15 ms and performs better at 50 ms.

Figure 6c describes the comparison of the vehicle's velocity to the packet delivery ratio regarding different BSM intervals. The velocity of the vehicles is inversely proportional to the packet delivery ratio. The ephemeral effect is observed in vehicles with high velocities and the packet delivery ratio performs better when the BSM intervals are kept at 50 ms. The packet delivery ratio decreases with a decrease in the intervals as more BSMs are generated frequently, which can cause congestion in the network.

Figure 7 shows the average routing delay alongside the number of packets that are being sent through the network. It is being observed that the most routing delay is incurred in the vouch algorithm, with the Grover and multi-BSM close to each other.



(**a**)

(**b**)

(**c**)

Figure 6. Multi-BSM evaluated in accordance with different intervals of BSM generations. (**a**) Average transmission delay vs. vehicle density. (**b**) Packet delivery ratio vs. vehicle density. (**c**) Packet delivery ratio vs. velocity.

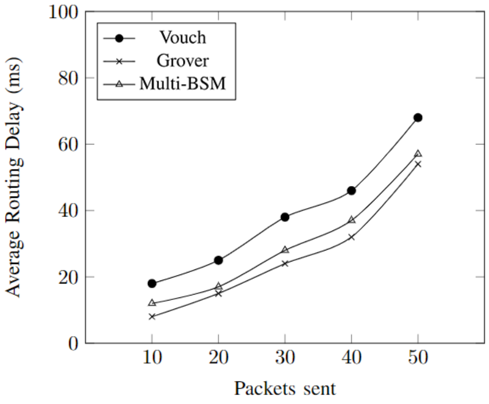


Figure 7. The comparison of average routing delays of the algorithms.

6. Conclusions

Position falsification attacks can be very dangerous; if they are not detected in the connected vehicular environment, they can cause minor mishaps to life-threatening incidents. In this paper, we proposed and evaluated the multi-BSM approach for the detection of anomalies, i.e., position falsification attacks, to be more precise. It was proven to be quite effective in detecting attacks. The multi-BSM also alerts the legitimate vehicles about the attacker present in the network even when the legitimate vehicle is not in the transmission range of the attacker vehicle. The RSUs demonstrate optimum real-time detection and prevention as they are equipped with better computational resources than those of vehicle

OBUs. All the RSUs are connected with each other and linked to a central database, which assures a better anomaly detection in real time. However, our work is limited to position falsification attacks at the current level, and we are not targeting other attacks that malicious attackers can initiate. This area has a lot of potential for future work.

7. Future Work

As discussed, there is a lot of potential for security aspects of vehicular communications. This paper targets position falsification attacks, but other attacks can also be handled by tweaking the mechanism to the respective attacks. The introduction of fog computing can also be of great service in this area instead of opting for cloud services. The V2X security credentials management and assessment are also relevant potential areas that the authors are currently exploring for future work.

Author Contributions: Writing—original draft, Z.T., S.S.S. and K.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by United Arab Emirates University (UAEU) Program for Advanced Research (UPAR) under grant number 31T122 and Zayed University Cluster grant number R20140.

Data Availability Statement: Not applicable.

Acknowledgments: This work was supported by United Arab Emirates University (UAEU) Program for Advanced Research (UPAR) under grant number 31T122 and Zayed University Cluster grant number R20140.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Al-Shareeda, M.A.; Anbar, M.; Hasbullah, I.H.; Manickam, S. Survey of authentication and privacy schemes in vehicular ad hoc networks. *IEEE Sens. J.* **2020**, *21*, 2422–2433. [CrossRef]
2. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Khalil, A.; Hasbullah, I.H. Security and Privacy Schemes in Vehicular Ad-Hoc Network With Identity-Based Cryptography Approach: A Survey. *IEEE Access* **2021**, *9*, 121522–121531. [CrossRef]
3. Al-Shareeda, M.A.; Manickam, S.; Mohammed, B.A.; Al-Mekhlafi, Z.G.; Qtaish, A.; Alzahrani, A.J.; Alshammari, G.; Sallam, A.A.; Almekhlafi, K. Provably Secure with Efficient Data Sharing Scheme for Fifth-Generation (5G)-Enabled Vehicular Networks without Road-Side Unit (RSU). *Sustainability* **2022**, *14*, 9961. [CrossRef]
4. Al-Shareeda, M.A.; Manickam, S.; Mohammed, B.A.; Al-Mekhlafi, Z.G.; Qtaish, A.; Alzahrani, A.J.; Alshammari, G.; Sallam, A.A.; Almekhlafi, K. Cm-cppa: Chaotic map-based conditional privacy-preserving authentication scheme in 5g-enabled vehicular networks. *Sensors* **2022**, *22*, 5026. [CrossRef] [PubMed]
5. Zaidi, T.; Faisal, S. An overview: Various attacks in VANET. In Proceedings of the 2018 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 14–15 December 2018; pp. 1–6.
6. Douceur, J.R. The sybil attack. In *Peer-to-Peer Systems, Proceedings of the First International Workshop, IPTPS 2002, Cambridge, MA, USA, 7–8 March 2002*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 251–260.
7. Hu, Y.C.; Perrig, A.; Johnson, D.B. Wormhole attacks in wireless networks. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 370–380.
8. Almalki, S.A.; Song, J. A review on data falsification-based attacks in cooperative intelligent transportation systems. *Int. J. Comput. Sci. Secur. (IJCSS)* **2020**, *14*, 22.
9. Kanchan, S.; Chaudhari, N.S. SRCPR: SignReCrypting proxy re-signature in secure VANET groups. *IEEE Access* **2018**, *6*, 59282–59295. [CrossRef]
10. Meyer, P.; Häckel, T.; Korf, F.; Schmidt, T.C. Network anomaly detection in cars based on time-sensitive ingress control. In Proceedings of the 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), Victoria, BC, Canada, 18 November–16 December 2020; pp. 1–5.
11. Othmane, L.B.; Dhulipala, L.; Abdelkhalek, M.; Multari, N.; Govindarasu, M. On the performance of detecting injection of fabricated messages into the CAN bus. *IEEE Trans. Dependable Secur. Comput.* **2020**, *19*, 468–481. [CrossRef]
12. Ji, H.; Wang, Y.; Qin, H.; Wang, Y.; Li, H. Comparative performance evaluation of intrusion detection methods for in-vehicle networks. *IEEE Access* **2018**, *6*, 37523–37532. [CrossRef]
13. Grover, J.; Gaur, M.S.; Laxmi, V. Position forging attacks in vehicular ad hoc networks: Implementation, impact and detection. In Proceedings of the 2011 7th International Wireless Communications and Mobile Computing Conference, Istanbul, Turkey, 4–8 July 2011; pp. 701–706.
14. Stabili, D.; Marchetti, M.; Colajanni, M. Detecting attacks to internal vehicle networks through Hamming distance. In Proceedings of the 2017 AEIT International Annual Conference, Cagliari, Italy, 20–22 September 2017; pp. 1–6.

15. Katragadda, S.; Darby, P.J.; Roche, A.; Gottumukkala, R. Detecting low-rate replay-based injection attacks on in-vehicle networks. *IEEE Access* **2020**, *8*, 54979–54993. [CrossRef]
16. Comert, G.; Rahman, M.; Islam, M.; Chowdhury, M. Change Point Models for Real-time Cyber Attack Detection in Connected Vehicle Environment. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 12328–12342. [CrossRef]
17. Negi, N.; Jelassi, O.; Chaouchi, H.; Clemençon, S. Distributed online data anomaly detection for connected vehicles. In Proceedings of the 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Fukuoka, Japan, 19–21 February 2020; pp. 494–500.
18. Petrenkov, D.; Agafonov, A. Anomaly Detection in Vehicle Platoon with Third-Order Consensus Control. In Proceedings of the 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia, 13–14 May 2021; pp. 463–466.
19. D'Angelo, G.; Castiglione, A.; Palmieri, F. A cluster-based multidimensional approach for detecting attacks on connected vehicles. *IEEE Internet Things J.* **2020**, *8*, 12518–12527. [CrossRef]
20. Berlin, O.; Held, A.; Matousek, M.; Kargl, F. POSTER: Anomaly-based misbehaviour detection in connected car backends. In Proceedings of the 2016 IEEE Vehicular Networking Conference (VNC), Columbus, OH, USA, 8–10 December 2016; pp. 1–2.
21. Gautham, P.S.; Shanmughasundaram, R. Detection and isolation of Black Hole in VANET. In Proceedings of the 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, India, 6–7 July 2017; pp. 1534–1539.
22. Leinmüller, T.; Schoch, E.; Kargl, F.; Maihöfer, C. Decentralized position verification in geographic ad hoc routing. *Secur. Commun. Netw.* **2010**, *3*, 289–302. [CrossRef]
23. Van der Heijden, R.W.; Al-Momani, A.; Kargl, F.; Abu-Sharkh, O.M.F. Enhanced position verification for VANETs using subjective logic. In Proceedings of the 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, Canada, 18–21 September 2016; pp. 1–7.
24. Boeira, F.; Asplund, M.; Barcellos, M.P. Vouch: A secure proof-of-location scheme for vanets. In Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, Montreal, QC, Canada, 28 October–2 November 2018; pp. 241–248.
25. Ranaweera, M.; Seneviratne, A.; Rey, D.; Saberi, M.; Dixit, V.V. Anomalous data detection in vehicular networks using traffic flow theory. In Proceedings of the 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, 22–25 September 2019; pp. 1–5.
26. Xiong, G.; Zhang, D.; Xu, J. An Effective Data Filtering Scheme Based on Context in VANETs. In Proceedings of the 2020 IEEE 20th International Conference on Communication Technology (ICCT), Nanning, China, 28–31 October 2020; pp. 752–756.
27. Haydari, A.; Yilmaz, Y. Real-time detection and mitigation of ddos attacks in intelligent transportation systems. In Proceedings of the 2018 21st International Conference on Intelligent Transportation Systems (ITSC), Maui, HI, USA, 4–7 November 2018; pp. 157–163.
28. Valentini, E.P.; Meneguette, R.I.; Alsuhaim, A. An attacks detection mechanism for intelligent transport system. In Proceedings of the 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 10–13 December 2020; pp. 2453–2461.
29. Alheeti, K.M.A.; Gruebler, A.; McDonald-Maier, K.D. On the detection of grey hole and rushing attacks in self-driving vehicular networks. In Proceedings of the 2015 7th Computer Science and Electronic Engineering Conference (CEEC), Colchester, UK, 24–25 September 2015; pp. 231–236.
30. Sultana, R.; Grover, J.; Tripathi, M. A Novel Framework for Misbehavior Detection in SDN-based VANET. In Proceedings of the 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), New Delhi, India, 14–17 December 2020; pp. 1–6.
31. Gu, K.; Dong, X.; Li, X.; Jia, W. Cluster-Based Malicious Node Detection for False Downstream Data in Fog Computing-Based VANETs. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 1245–1263. [CrossRef]
32. Li, F.; Guo, Z.; Zhang, C.; Li, W.; Wang, Y. ATM: An active-detection trust mechanism for VANETs based on blockchain. *IEEE Trans. Veh. Technol.* **2021**, *70*, 4011–4021. [CrossRef]
33. Wang, W.; Luo, T. The minimum delay relay optimization based on nakagami distribution for safety message broadcasting in urban VANET. In Proceedings of the 2016 IEEE Wireless Communications and Networking Conference, Doha, Qatar, 3–6 April 2016; pp. 1–6.
34. Wang, J.; Chen, H.; Sun, Z. Context-Aware Quantification for VANET Security: A Markov Chain-Based Scheme. *IEEE Access* **2020**, *8*, 173618–173626. [CrossRef]
35. Kumar, G.; Saha, R.; Rai, M.K.; Kim, T.H. Multidimensional security provision for secure communication in vehicular ad hoc networks using hierarchical structure and end-to-end authentication. *IEEE Access* **2018**, *6*, 46558–46567. [CrossRef]
36. Varga, A.; Hornig, R. An overview of the OMNeT++ simulation environment. In Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops, Marseille, France, 3–7 March 2008; pp. 1–10.
37. Krajzewicz, D.; Erdmann, J.; Behrisch, M.; Bieker, L. Recent development and applications of SUMO—Simulation of Urban MObility. *Int. J. Adv. Syst. Meas.* **2012**, *5*, 128–138.
38. Sommer, C.; German, R.; Dressler, F. Bidirectionally coupled network and road traffic simulation for improved IVC analysis. *IEEE Trans. Mob. Comput.* **2010**, *10*, 3–15. [CrossRef]