*electronics*

MDPI

*Article*

# Real-Time Detection of DoS Attacks in IEEE 802.11p Using Fog Computing for a Secure Intelligent Vehicular Network

**Samuel Kofi Erskine and Khaled M. Elleithy ***

Computer Science and Engineering Department, University of Bridgeport, Bridgeport, CT 06604, USA
* Correspondence: elleithy@bridgeport.edu; Tel.: +1-203-576-4703

Received: 6 June 2019; Accepted: 5 July 2019; Published: 11 July 2019

**Abstract:** The vehicular ad hoc network (VANET) is a method through which Intelligent Transportation Systems (ITS) have become important for the benefit of daily life. Real-time detection of all forms of attacks, including hybrid DoS attacks in IEEE 802.11p, has become an urgent issue for VANET. This is due to sporadic real-time exchange of safety and road emergency message delivery in VANET. Sporadic communication in VANET has the tendency to generate an enormous amount of messages. This leads to overutilization of the road side unit (RSU) or the central processing unit (CPU) for computation. Therefore, efficient storage and intelligent VANET infrastructure architecture (VIA), which includes trustworthiness, are required. Vehicular Cloud and Fog Computing (VFC) play an important role in efficient storage, computation, and communication needs for VANET. This research utilizes VFC integration with hybrid optimization algorithms (OAs), which also possess swarm intelligence, including Cuckoo/CSA Artificial Bee Colony (ABC) and Firefly/Genetic Algorithm (GA), to provide real-time detection of DoS attacks in IEEE 802.11p, using VFC for a secure intelligent vehicular network. Vehicles move ar a certain speed and the data is transmitted at 30 Mbps. Firefly Feed forward back propagation neural network (FFBPNN) is used as a classifier to distinguish between the attacked vehicles and the genuine vehicles. The proposed scheme is compared with Cuckoo/CSA ABC and Firefly GA by considering jitter, throughput, and prediction accuracy.

**Keywords:** Cuckoo/CSA (ABC); Firefly/Genetic Algorithm (GA); Vehicular Cloud and Fog Computing (VFC); DoS attacks; IEEE 802.11P; VANET; ITS

## 1. Introduction

VANET is a popular, modern network. The network is termed an ad-hoc network, as the position of the vehicles changes at every instant of time. The average speed of vehicular nodes varies from 40 to 80 km/h [1]. Due to this high randomness in location, VANET is quite prone to security threats, especially hybrid DoS attacks, including all forms of attacks. Uncertainties, such as hybrid DoS attacks, are the biggest reasons for security threats. VANET utilizes vehicles as mobile nodes in the form of a sub-class of a mobile ad-hoc network (MANET) to communicate with nearby vehicles and among vehicles close to roadside units (RSUs) or equipment, though is differs from other networks according to its characteristics [2]. Particularly, the vehicles (nodes) are inadequate for the road topology when moving; thus, vehicles' future positions can be predicted when information of the road is available. As per IEEE 1471-2000 and ISO/IEC 42010 framework general guidelines, VANET systems can be categorized into three domains, including mobile, infrastructure, and generic domains [3].

Figure 1 depicts the VANET infrastructure architecture (VIA). The mobile domain transfers the information and communicates with the infrastructure domain. It utilizes IEEE 802.11p beacons and signals, which process the data and proceed towards modulation [4]. Then, the infrastructure domain communicates with generic domains and then exchanges the information. The flows of data between the mobile and stationary resources results in effective utilization of the road with the user, which utilizes IEEE 802.11p beacon communication standard.

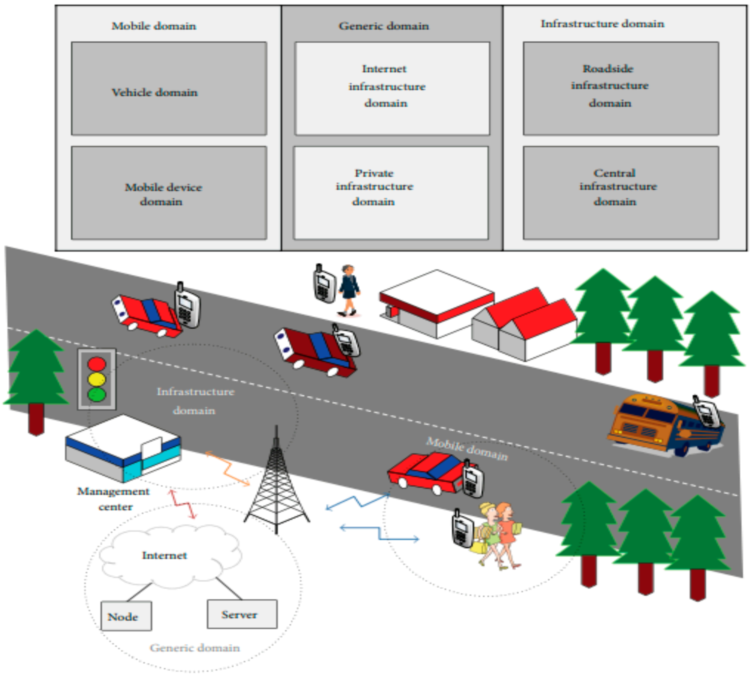


**Figure 1.** The vehicular ad hoc network (VANET) Infrastructure Architecture (VIA). The mobile domain is composed of two parts. The infrastructure domain also consists of two parts. The generic domain has private and internet infrastructure. It can be defined in the form of varied nodes with servers and varied computing resources operating directly or indirectly for VANET.

In this research, the transmission rate of information for real-time IEEE 802.11p information delivery in VANET is 30 Mbps. Vehicles move in groups, as they are directed in the VIA to their intended destination (as shown in Figure 1). In the VIA also, vehicle cooperation in the group movement is such that they exchange frequent sporadic broadcasts of safety messages. These broadcasts carry the information of the speed of the vehicle and their position, whilst utilizing the IEEE 802.11p beacon's dedicated channel [5]. During normal operation of the IEEE 802.11p medium access control (MAC) protocol random access specification, beacon loss is possible. This can be attributed to impairment of wireless channels (i.e., beacon transmissions overlapping resulting from several vehicles, which can lead to collision/congestion). Collision/congestion (CC) can be reduced based upon proper selection of MAC protocol real-time transmission methods, which include secure authentication and key distribution algorithm models, and secure transmission range models, which can be deployed in the VIA network. Based upon this, performance parameters, such as real-time end-to-end delay sensitivity for trust enforcement of neighboring nodes in VANET, can be measured [6,7].

Nevertheless, it is possible that the IEEE 802.11p beacon transmissions can also get corrupted through malicious attacker vehicles. They may also present themselves in all forms of attacks, including hybrid DoS attacks (HDSA), which include DoS jamming signal attack, (DoD JSA), packet drop (PD), and resources consumption/RSU or CPU overutilization (RCRCO) [8]. The VANET safety can seriously be at risk, since vehicles would not be capable of properly utilizing the information obtained. However, vehicles are required to utilize and transmit the information based upon the IEEE 802.11p beacon's relay through the RSU in order to sensitize awareness in VANET. The RSU utilizes the information to also update other vehicles about the requirements of end-to-end delay and jitter in the network, which is imposed by the automotive control system (ACS) from the traffic management center, as shown in the VIA in Figure 1.

Consequently, real-time detection of all forms of attacks, including hybrid DoS attacks (HDSA), require trustworthiness, intelligent computation, and efficient storage, which can be achieved through vehicular cloud and fog computing (VFC). These can provide trustworthiness in VANET. In addition, integration with hybrid deployment of optimization algorithms (OAs) in VANET also provides swarm intelligence. The OAs include Cuckoo/CSA (ABC), and Firefly/Genetic Algorithm (GA). These OAs can also be integrated with authentication and KDE mechanisms. This integration with the real-time detection of HDSA can provide secure methods in the MAC layer, which in turn can be used to mitigate all forms of attacks, including HDSA, such as DoS JSA, PD, and RCRCO, which utilizes IEEE 802.11p beacon transmissions in VANET. This represents an urgent practical problem that we are motivated to investigate in this research.

### *1.1. Background Study of This Research*

Real-time detection of only DoS JSA using IEEE 802.11 signal in VANET was proposed and investigated based upon previous studies [9,10]. In these studies, the MAC layer misbehavior of some vehicles and nodes violates IEEE 802.11 rules. Small back-off counters were chosen to access the channel more frequently than other nodes. However, their performance were degraded. In these investigations, however, restriction in detection of all forms of attacks, including HDSA, was an issue. Moreover, the investigation was based on only a DoS JSA attack. In detecting DoS JSA only in VANET, the method in a previous study [11] that utilized a unicast traffic method based upon the regression model was proposed. However, the proposed method did not consider any trustworthiness investigation of the nodes in the network. Real-time detection of DoS attacks in the IEEE 802.11p vehicular network method was also proposed in a previous study [12]. This considered beacons transmission regularly in IEEE 802.11p in broadcast mode only, without retransmission. This method also included an alternative jamming detector for considering detection of only DoS JSA attacks in a VANET platoon. However, the investigation revealed gaps in trustworthiness in the protocol. Based upon the investigation of these two or more methods, we can verify that the DoS attacks considered for investigation in VANET were based only on DoS JSA. There are other forms of attacks eminent in VANET, which include HDSA. The detection of all other attacks and HDSA still presents the greatest challenge in VANET safety application deployment. In addition, there are other forms of DoS attacks, such as PD, RCRCO overutilization, and DoS resilience attacker (DRA). These attacks altogether also form HDSA [13], which mostly cause overutilization of the RSU. However, none of the above defined proposed schemes in VANET considered investigation for detecting HDSA, which also includes DRA. Moreover, the authors' investigations concerning utilizing the above proposed schemes demonstrate only limited recommendation and provision for trusting methods, secure efficient storage mechanisms, proper OAs, and authentication and KDE methods based upon the investigations of the proposed schemes. The authors detected only DoS JSA based upon the investigations of their proposed schemes. DoS attacks encompass DRA for the sake of this research. Therefore, it is important to investigate HDSA using a sophisticated approach. This new approach will be capable of detecting all forms of DoS attacks, including HDSA attacks, which should be supported in this research.

Vehicular Cloud and Fog Computing (VFC) is a standard that comprehends FC and vehicular cloud (VCC) [14]. VFC is also a solution that satisfies the requirements of VANET, such as secure and efficient computing, storage, and in-network resource provision [13]. In addition, optimization algorithms (OAs), such as Cuckoo/CSA (ABC) [15], Firefly algorithm (GA) [16], and firefly neural algorithm [17] are capable of providing swarm intelligence. The OAs are either heuristic or metaheuristic in nature and have problem-solving skills. They also have the capability to adjust DoS JSA and HDSAs (i.e., congestion and collusion), which include all other forms of attacks, such as DoS JSA, PD, and RCRCO, for optimum user experience [18]. The OAs have also been used to evaluate a real-time data transmission in VANET [19], which utilized IEEE 802.11p for dedicated short-range communication

(DSRC) technology. VFC integration with OAs and trust detection of the nodes in VANET, which also utilize authentication/KDE in VANET, can appropriately secure the VANET through the RSU. This secure method for VANET protection provide a real-time detection of DoS attacks in IEEE 802.11p, which utilizes the DSRC technology. It also provides the safety of roads and highways based upon intelligent transportation system (ITS) opportunities. Therefore, real-time detection of DoS JSA and HDSA utilizing IEEE 802.11p, which is based upon VFC, requires investigation to evaluate end-to-end delay and jitter in VANET, due to DoS JSA and HDSA attack, (congestion and collision) for trust evaluation.

The authors in previous studies [14–16] have conducted investigations separately using Cuckoo/CSA (ABC) and Firefly Genetic Algorithm (GA), respectively. The investigations were performed to evaluate delay sensitivity for real-time detection for only DoS JSA attacks in VANET, which also utilized DSRC technology. However, based upon the investigation conducted with the Cuckoo/CSA (ABC) scheme, it revealed that it was not centered on VFC. In addition, most of the schemes' investigations dwell on only the unicast method for data transmission. However, this method did not achieve trustworthiness in the network. The authors have conducted an investigation on Firefly (GA), and utilized the concept of VANET as key enabler of future ITS, utilizing real-time detection of DoS attacks. The authors also trained the misbehavior of the nodes on the paths of vehicles delayed in VANET. They also utilized the DSRC technology and multicast data transmission. However, the author's investigation was limited. This is based upon the fact that the investigation does not include all forms of attacks, including HDSA attacks, such as DoS JSA, PD, and RCRCO, in the network. In addition, the absence of the VFC method was also a major limitation observed in the schemes. Therefore, it can be concluded that there is a trustworthiness limitation in VANET. This still presents the greatest challenge.

To address these challenges in VANET, in this paper we consider all forms of attacks, including all forms of DoS attack detection in VANET, which includes but is not limited to DoS JSA, HDSA (congestion and collusion), PD, and RCRCO/DoS attacks in our proposed scheme VIA models. We also consider the hybrid deployment of OAs with VFCs and integrate full authentication/KDE trust mechanism deployment in the VANET. These will be used to evaluate the end-to-end delay and jitter in real-time IEEE 802.11p hybrid multicast and unicast data transmission in VANET. Therefore, in this paper we propose real-time detection of DoS attacks in IEEE 802.11p using VFC in a Secure Intelligent Vehicular Network.

### *1.2. Research Contribution*

The main contributions of this research are:

- Deployment of trust in VANET utilizing VFC and hybrid integration of OAs, which include Cuckoo/CSA (ABC) and Firefly (GA) with authentication/KDE. VFC provides a search space for information processing and achieves efficiency in computational overhead due to advantages in rapidly stored vehicular information processing using the V2V and V2RSU, and RSU2FS communication behavior in this research.
- Real-time detection of all forms of attacks, including HDSA attack detection, such as DoS JSA, PD, and RCRCO in VANET, to provide trustworthiness in the network.
- Provision of IEEE 802.11p benefits information processing. which utilize hybrid multicast and unicast broadcast data transmission in VANET for efficient and real-time transmission of safety information.
- Provision for single next hop vehicle (SNHV) probability analysis for efficient data processing within the elliptical segment area transmission range (ESATR) in VANET.
- Provision for regression model prediction based upon reduced delay and jitter in VANET for secure road safety provision.

The rest of the paper is organized as follows. Section 2 presents the related work. Section 3 presents the secure real-time detection of DoS attack models (DAM) and jamming signal attack models (JAM). Both attack models provide Hybrid DoS attack model (HDAM) prevention mechanisms in VANET. Section 4 presents the preventive mechanisms and the system models, including the system architecture model (SAM) and elliptical segment area transmission range model (ESATRM), OA deployment, and trustworthiness of nodes of the proposed scheme. Section 5 presents the resulting analysis and discussion. Section 6 is a miscellaneous section for background study comparison of VANET protocols, and Section 7 presents the conclusions.

## 2. Related Work

This section discusses related work in VANET. The section is also categorized into two subsections, which are Sections 2.1 and 2.2. Section 2.1 includes securing VANET-Centralized Architecture based on HDSA, including other related attacks. Section 2.2 includes securing the VANET-Fog Computing Centric Architectures, as follows.

### *2.1. Securing VANET-Centralized Architecture Based on DoS Attacks and Other Related Attacks*

In a previous study [20], the authors proposed malicious node detection on vehicular ad-hoc networks. They used Dumpster Shafer theory to investigate DoS attacks. However, during the investigation it was discovered that it was not centered on secure storage solutions. In addition, hybrid multicast and unicast data transmissions were not used to investigate for real time detection of all forms of attacks, including HDSA attacks. Instead, the authors' investigation was centered on an artificial neural network-based technique, which used a self-organized map. In the investigation, the authors also used only a trace file to train the network, which works as an input to self-organize the map. This was in order to provide supervised learning to their network. Although, the authors used a self-organized map (SOM) classifier for detection of misbehavior nodes; the method used was not fully investigated or explained. Moreover, there were also limitations in investigation of the IEEE 802.11 standard data transmission technique. The IEEE 802.11 utilizes the DSRC technology to investigate communication of vehicles in the network. This is observed as a major limitation of the scheme. In a previous study [21], the authors proposed prevention of DoS attacks over a vehicular ad hoc network using a quick response table. However, based upon the proposed scheme, there was a limitation. This includes use of a clear security method that was required to secure the network. This requires urgent attention. Another limitation observed for the scheme was that the authors did not conduct an investigation regarding an efficient storage mechanism for the network deployment. In addition, there was no recommendation for any trustworthiness method, which would be used to secure the network. In addition, the detection of DoS attacks was only based upon certain forms of attacks, such as gray hole, Sybil, and black hole attacks only. However, these attacks are of different categories. Thus, the authors' investigation could not be considered appropriate, due to absence of investigation of DoS JSA, PD, and RCRCO overutilization, which relates mostly to the trustworthiness and efficient provision of data for RSU in VANET. However, it was discovered in the authors' investigation that the proposed security mechanism was merely a discussion method for routing in VANET. The routing method was only used to identify and eliminate the existing security threats. The authors did not recommend any real-time investigation of the methods used for investigation of trustworthiness in VANET.

In a previous study [22], the authors proposed an efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks (ELIDV). From the perspective of the authors, they designed and implemented ELIDV with the aim of protecting the network from only three kinds of attacks, namely DoS attacks, integrity targets, and false alert generation. In addition, the proposed ELIDV security method was also based upon a set of rules that detected malicious nodes promptly. However, the proposed method was not evaluated based upon high prediction accuracy evaluation of HDSA for VANET. Also, the authors' investigation concerning secure method provision in VANET was without consideration for any efficient storage mechanism. Therefore, it can be concluded that there was no trustworthiness protection provision in the network. In addition, another limitation that was discovered was that the DoS attack detection method used was not centered on any HDSA, including DoS JSA, PD, or RCRCO overutilization. The proposed scheme was also identified as having a limitation in designing a secure encryption and authentication mechanism. This would otherwise be used for providing a hybrid investigation of DoS attacks that would also include investigation of real-time data transmission in VANET. In a previous study [23], the authors proposed detection and prevention mechanisms of distributed denial of service (DDoS) attacks in VANETs. Based upon the proposed scheme, the authors concentrated only on DDoS attack detection and the prevention scheme. The basic principle of the scheme relied only on keeping track of the number of packets injected into the network. The authors claimed that the proposed scheme did not include any communication overhead (CO) that would affect the network resources. Nevertheless, there were limitations in the network, which included lack of provision of any efficient storage mechanisms; these would be used to secure the network, however, they were not investigated in the proposed scheme, which can lead to CO. Therefore, trustworthiness was an issue with the proposed scheme. In addition, due to the limitation of trustworthiness in the network, CO was increased in the proposed scheme. Another limitation observed with the proposed scheme was the unavailability of hybrid security method investigation. This would be used for detection of all forms of attacks, including HDSA attacks in the network. Therefore, we can verify that the proposed scheme would incur DoS JSA, PD, and RCRCO, which affects the RSU secure information processing in the network. In addition, the proposed scheme performance evaluation was not based upon end-to-end delays in the network, which requires urgent attention.

The authors in another study [24] proposed a review of the intrusion detection system (IDS). A survey of IDS, based upon DoS attacks, has been provided with the examination and comparison of every technique, with advantages and disadvantages. Few guidelines have been presented for the development of IDS with prospective application in VANET-cloud and fog computing (VFC). The objective of the authors was the identification of open challenges, leading trends, and future research in IDS deployment in the network. Bridging the gaps by means of overhead detection rate and performance, the authors proposed a proactive bait with respect to the honeypot optimized system. However, leading to the discussion of the authors proposed scheme, no investigation in network performance metric evaluation of end-to-end delay, throughput, and prediction accuracy performance of the proposed scheme were evaluated. Based upon another limitation that was identified, the proposed scheme did not include secure method and storage mechanism investigation, which was also a major concern. Therefore, trustworthiness and accurate processing of safety information in VANET was also a concern. Exploring further investigation in VANET based upon VIA infrastructure, using Vehicular Cloud and Fog Computing (VFC), is important and the investigation below is based upon the concept of VFC.

### *2.2. Securing the VANET-Fog Computing (VFC) Using Cloud-Centric Architectures*

The authors in a previous study [25] identified the security goals for vehicular cloud computing (VCC); also known as VFC) interoperability. The authors provided an Authentication and Key Agreement (AKA) framework for VCC. Particularly, the authors proposed the problems with the challenges for the design of consistent AKA with extra strong security assurance for VCC. A hybrid AKA framework has been proposed, which combines “single server, 3-factor protocol” with “non-interactive, identity-based, key established protocol” and computed the performance on the basis of the simulated platform. The authors in a previous study [26] introduced a novel method for serving speed-based lane changing, time of arrival (TOA), and collision avoidance on the basis of localization in VANET. TOA has been designed for those areas in which there is an unavailability of GPS signals. The design of TOA provides clear line of sight for exact services for localization and positioning applications. The authors addressed collision avoidance with automatic braking and camera-based surveillance. The viability and feasibility of the algorithms were established via simulation in Simulation of Urban Mobility

(SUMO) and Network Simulator (NS-2). The authors designed an mobile application interface (MAI) for the onboard unit for effective, smart monitoring of remote traffic.

The authors in a previous study [27] proposed an exclusive hierarchy for cache discovery with a review on co-operative caching methods in VANET with the classification of linked cache discovery methods in the classification. According to this, the authors used varied cache discovery methods and examined the potential for addressing the appropriate challenges that occurred, while also deploying a non-safety application in VANET, which avoided the common pitfalls. The future lies in the utilization of this research for the development of new co-operative caching methods, such as fog computing, which could offer enhanced performance in VANET, while comparing the traditional approaches on the basis of co-operative caching methods. The authors in a previous study [28] presented the VANET design architecture for authentication key delivery with less delay between vehicles with more mobility, utilizing fog as well as cloud computing. The authors introduced fog computing for the extension of cloud computing, with the context of a middle fog layer among cloud and mobile devices for the production of varied benefits. As the keys are produced directly from the middle layer, the latency is significantly diminished. Additionally, the amount of message exchanges among vehicles varied in VANET as elements lessened, as compared to traditional methods. Accordingly, the resultant system was more effective. The design was executed and validated by a network simulation tool for a single as well as a multi-vehicle system.

In another study [29], the authors presented a novel technique to address the problem of data sharing and delegated the data management to a trusted third party (TPA) on the basis of a bilinear pairing method. For the achievement of this goal, the authors utilized fog computing as the major tool for a utility computing hypothesis for storage of a large amount of data and executed the re-encryption procedure safely. Varied resources, such as an on-board unit, communication, endless battery life, and computing are implanted in the vehicles for usage for the enhancement of an intelligent transportation system (ITS). The main challenge for VANET is to safely distribute the significant information between the vehicles. In a few cases, the owner of the data was not accessible and could not control the process of data-sharing with the novel user or revoke the traditional user. The authors in another study [30] used Firefly (genetic algorithm (FA)) to investigate vehicles that travelled along highways that encountered some form of VANET attacks. These vehicles that were deployed in the VANET were vulnerable due to DoS attacks which caused delays in the network. Afterwards, the authors utilized a clustering algorithm to facilitate good communication links, however, VFC was a limitation for the network. In another study [31], the authors proposed a new unicast routing protocol for a vehicular network. The protocol was based upon two techniques: clustering algorithm technique, which played a role in organizing and optimizing the exchange of routing information based on quality of service requirement, and the artificial bee colony Cuckoo (ABC) algorithm, which was used to find the best route path from the source to the destination. This complied with measuring the delay and jitter in the network. However, investigation of the network for trust was not based upon HDSA. In addition, only multicast data transmission was a limitation, including absence of VFC. Therefore, further investigation and evaluation of delay and jitter in VANET is important.

The authors in another study [32] proposed a scheme for Sybil attack prevention through an identity symmetric encryption scheme in vehicular ad hoc networks. The authors' investigation also included DoS attacks and all other forms of attacks, such as spoofing and identity disclosure. Based upon the proposed protocol, a novel lightweight approach for preventing all these many forms of attacks, including Sybil attacks and DoS attacks in VANET, was proposed by the authors. The scheme used symmetric key encryption and authentication between RSUs and vehicles on the road. The intent was to prevent malicious vehicles and nodes from obtaining more than one identity inside the network. However, the proposed scheme did not require management in RSUs or certification authority (CA). The scheme only utilized a minimum amount of message exchange with the RSU, with the authors insisting the scheme was effective. However, based upon the network deployment, some vehicles did not share information. Vehicles sent fake requests and caused breakdowns, leading to trustworthiness concerns in the network.

The work proposed in a previous study [33], which included early DoS attack detection in VANET, used an attacked packet detection algorithm (APDA) for vehicles. The vehicle represents mobile nodes equipped with an on-board unit (OBU) that allows them to send and also receive messages from the other nodes in the VANET. The messages successfully reached the intended destination without any interruption. In another study [34], the authors discussed DoS attacks in VANET and used the Bloom-filter-based detection method, which provided service availability for legitimate vehicles or nodes in the network. A series of attacks were encountered in the network that caused a communication break. This is due to DoS JSA, source sink attacks, and all other forms of attacks, including HDSA, which were left uninvestigated.

Based upon the above descriptions and investigations, it can be reasoned that real-time detection of DoS attacks, which utilized IEEE 802.11p deployment in VANET using the DSRC technology, was an issue. Thus, secure method evaluation, including VFC and optimization algorithms, were mainly issues that were left uninvestigated by the authors. This is based upon the fact that they found the investigation of various proposed schemes in VANET complex to carry out. Also, it was determined in the investigation that VFC was a major design issue in VANET. Hybrid method investigation deployment limitations persist. In addition, most of the proposed schemes' investigation limitations revealed trustworthiness and secure storage mechanism concerns, and absence of hybrid optimization algorithm deployment, which would be required to evaluate network performance metrics, such as end-to-end delay and jitter in the network.

Moreover, most of the schemes proposed by the authors that were based upon storage mechanisms for processing of information, as discussed previously, focused on either using only unicast, multicast, or broadcast methods to assess VANET information, processing performance metrics with the RSU. None of the proposed schemes considered hybrid unicast and multicast or broadcast and secure authentication/KDE deployment methods for investigating all forms of attacks, including HDSA. However, these limitations are a major concern that require further investigation in VANET in order to process safety and emergency message delivery in VANET. Thus, the authors of the above proposed schemes utilized insufficient end-to-end delay measurement methods, as discussed in Sections 2.1 and 2.2 for VANET (VIA), for real-time detection of HDSA.

## 3. Secure Real-Time Detection of DoS Attacks, Prevention Measures in VANET

### *3.1. Hybrid DoS Attacks (HDSA)*

Hybrid DoS attacks (HDSA) employ HDSA models. These models are designated as the proposed scheme attack models. They also encompass all of the attack models that mitigate DoS JSA, PD, and RCRCO (DoS attack/RCRCO) attacks. These attacks should be identified and mitigated in the VIA system architecture models, which include the proposed scheme system architecture model (PSAM) and the proposed scheme elliptical segment area transmission range models (PESATRM). These models utilize the attacked packet detection algorithm (APDA) to identify and mitigate HDSA and DoS JSA, including other attacks in the network (these models will be explained further in subsequent Sections 3 and 4 as needed). However, before we proceed on, it is important to initially understand the DoS attack/RCRCO model, since it serves as the main target attack point investigated in the proposed scheme of this research.

### *3.2. DoS Attacks and Model*

Denial-of-service (DoS) attacks block the availability of computing systems and network services. Therefore, the DoS attack model is needed to mitigate these attacks. DoS attacks also overwhelm the network with excessive traffic through the channel with naturally generated messages. The computing system and network services crash. In addition, they are unable to operate as accurately and effectively as required. The computing system also denies services to legitimate users [35]. In addition, as a substitute to the system to functioning appropriately, it would rather perform other irrelevant functions not required in the network.

All forms of DoS attacks, including HDSA model attacks such as DoS JSA, PD, and RCRCO/DoS attacks, can be experienced through inside and outside malicious intruders in the network. These halt provision of network availability to its real users. This occurs through flooding of the control channel with naturally generated illegal and malicious messages sent at a high speed [12]. DoS attack/RCRCO key resources include high bandwidth demands, CPU and RSU overutilization, and excessive memory computation. DoS attack/RCRCOs have a tendency to reduce the speed and volume of the legitimate network by consuming high bandwidth resources. Through DoS attack/RCRCOs, packet processing and network devices can be prevented from responding to management requests. This can effectively lock the devices by consuming excessive memory, leading to CPU and RSU overutilization of resources.

Figure 2 depicts a DoS attack model (DAM), which is also an aspect of the HDSA model used in this research. DAM include vehicles that have experienced all forms of attacks, including HDSA. When DoS attack/RCRCOs occur, they result in accidents at locations X and Y. Another scenario of DoS attack/RCRCO includes high bandwidth CPU and RSU overutilization and high memory computation, which also leads to broken signals. Since vehicles cannot appropriately utilize the 802.11p beacons for message transmission, this leads to collision and congestion of other vehicles. Consequently, this also leads to an encounter of broken IEEE 802.11p beacon signals. This act also leads to not being able to fully acquire the IEEE 802.11p beacons and signals, which results in end-to-end delays to the network. Moreover, packet drop (PD), false information (FI), and jamming signal attacks (DoS JSA) occurrence in VANET is possible. In the other scenario, normal vehicles that are travelling to their intended destinations communicate with other vehicles. The vehicles utilize the unbroken 802.11p beacons and signals, which encompass V2V, V2RSU, and RSU2RSU communication. Based upon this scenario, the RSU and fog server connection is achieved through either wired means or by wireless means. The connection of the RSU and FS utilizes the unbroken 802.11p beacons and signals with the road-side unit to vehicle (RSU2V) communication and vehicle to road side unit (V2RSU) communication to process information in the network.

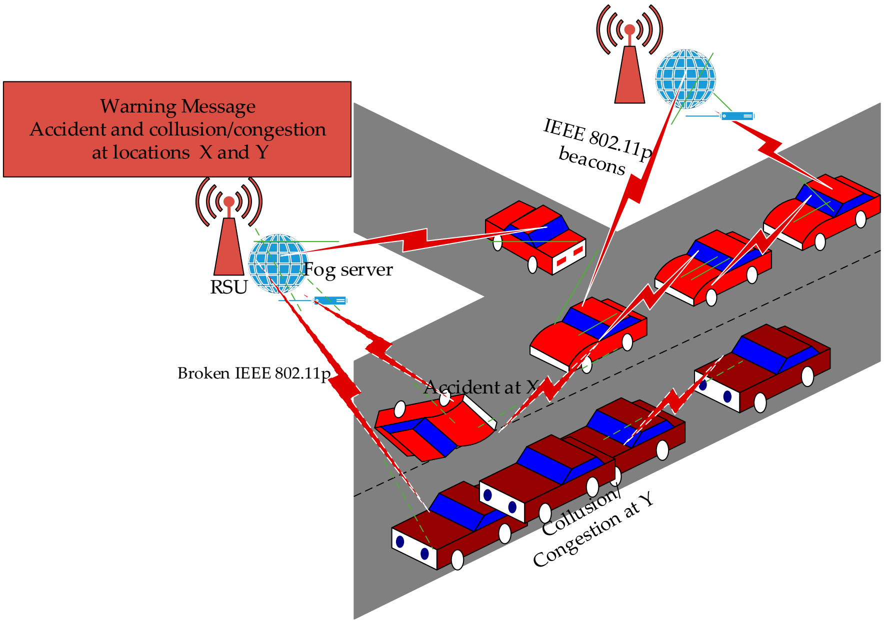


**Figure 2.** DoS attacks model (DAM).

The RSU2V, V2RSU, and V2V effective signal communication of the unbroken IEEE 802.11p beacons and signals can also be achieved through the fog server (FS) effective connection with the

RSU. These effective connections, which are secure, utilize the IEEE 802.11p beacons and signals generated from the accident scenarios to sensitize awareness of the road conditions. The scenario of the vehicle information delivery may also represent congestion and collision of vehicles that are used as a standard for safe information dissemination to other vehicles and road users. Based upon this, all other normal vehicles that have not yet encountered congestion, collision, or accidents will appropriately be informed about any accident and collision or congestion situation that have occurred. An example is accidents and congestion and collisions situation that have occurred, such as at locations X and Y in Figure 2. Moreover, the broken IEEE 802.11p beacons and signals are intended to cause end-to-end delay in the VANET, which requires evaluation of network performance metrics. When accidents occur, they prevent timely relay of the IEEE 802.11p beacons, leading to PD, FI, and DoS JSA. Therefore, through this research, we launch further investigation to evaluate the presence of all forms of attacks, such as HDSA, and including PD/FI and DoS JSA, using attacked packet detection algorithms. Anticipation of the implementation of the proposed scheme system architecture model (PSAM) is needed. This will be used to detect attacked packet drop PD/FI and DoS JSA scenarios. This is also an important component of this research, whereby HDSA model requirements should be investigated for VANET. Now, it is important to understand the effects of PD/FI and DoS JSA, which also utilize the HDSA model.

### 3.3. Packet Drop (PD) and False Information (FI)

A packet drop (PD) DoS attack (PDA), including FI, is one of the attacks that originates from the HDSA model. It may occur due to interference of 802.11p beacons that may be present in the PSAM. PDA may also lead to end-to-end delay of path detection of the communication process in VANET, during the deployment of V2V, V2RSU, and RSU2V communication in the network. On the other hand, PDA will also lead to FI message delivery in VANET. FI may also represent incorrect or fake information generated through packet drop (PD), which may have resulted from all forms of attacks, including DoS attacks. Thus, PDA might be sent purposefully by a node to another node in the network that has the tendency to create congestion/collision (CC) traffic scenarios. This may also lead to misinformation of the actual road and traffic situation information prediction accuracy. Usually, when PD and FI are encountered in the network, they will also lead to generation of falsified information. Drivers or road users would usually leave the road due to PDA and DoS JSA, since the road becomes available for attackers to exploit for their own purposes. Therefore, it is important that DoS JSA should also be considered for investigations in the PSAM.

### 3.4. DoS Jamming Signal Attack (DoS JSA)

DoS jamming signal attacks (DoS JSA) represent a high form of DoS attacks that have been investigated mostly by researchers. They are also a component of the HDSA model proposed in this research. During DoS JSA encounters, the attacker usually jams the channel, which can be represented as the congestion/collision scenario in VANET. The main objective of DoS JSA is for a jammer to trick a legitimate IEEE 802.11p beacon's signal communication, and reduce or degrade the overall VANET performance. During the DoS JSA encounter, network users are not permitted to access the network. This usually causes broken IEEE 802.11p beacon signals and introduces end-to-end delays in the network. Jammers or DoS JSA also have an objective of causing packet dropping in the network. DoS JSA strategies include introducing deceptive DoS JSA (DDJA), reactive DoS JSA (RDJA), random DoS JSA (RADJA), and constant DoS JSA (CDJA). Semi-valid packets are transmitted through DDJA. Through the DDJA, the packet header of the information becomes valid, whilst the payload may not be used. With CDJA, the IEEE 802.11p beacon's radio signals continue to be emitted.

With reactive RDJA encounters in VANET, resources are wasted and the receiver is targeted when more noise encounters in the data packet occur. RADJA effects can be experienced in two modes. In the first mode RADJA leads to excessive traffic encounters of traffic for random, intermittent periods of time, whereas in the second mode, RADJA leads to transmission of the signal being stopped for random, intermittent time frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSP) [36].

Figure 3 represents vehicular communication of the DoS jamming signal attack model (DJSAM) scenario of the proposed scheme. This also serves as a component of the HDSA model (HDAM). In the figure there are two scenarios. In the first scenario there are normal vehicles that utilize the IEEE 802.11p unbroken signals. The unbroken signals are also utilized to initiate V2V communication to sensitize each vehicle to safety information for the roads, and the DoS JSA situation that has occurred. This can be achieved through the connection of the RSU, which is either wired or wirelessly connected with the fog server (FS). This connection arrangement is used to disseminate road emergency situation information concerning accidents and road safety conditions. In the second scenario, the vehicles are designated to communicate within an elliptical segment area (ESA). The ESA represents a region where vehicles that are moving within a specified communication range encounter an actual channel DoS JSA situation in the network. The second scenario also includes utilizing the IEEE 802.11p broken signals. The broken signal communication scenario incurs unacceptable end-to-end delays in the network through V2V, V2RSU, and RSU2V communication that also convey the DoS JSA condition information of the road to other vehicles. However, due to the fact that DoS JSA has already been discussed previously, investigation of end-to-end delay on the path of each vehicle in the network would be needed. This requires using sophisticated system architecture models, such as the proposed PSAM scheme (which will be explained shortly). The PSAM is required to utilize attacked packet detection algorithms combined with the HDAM model. This would be beneficial to use to detect the end-to-end delayed path of all HDAM attacks, including DoS JSA, PD, RCRCO, and all forms of associated attacks in the network that have the capability to introduce end-to-end delay and jitter. The HDAM implementation will be explained in the prevention mechanism and the PSAM.

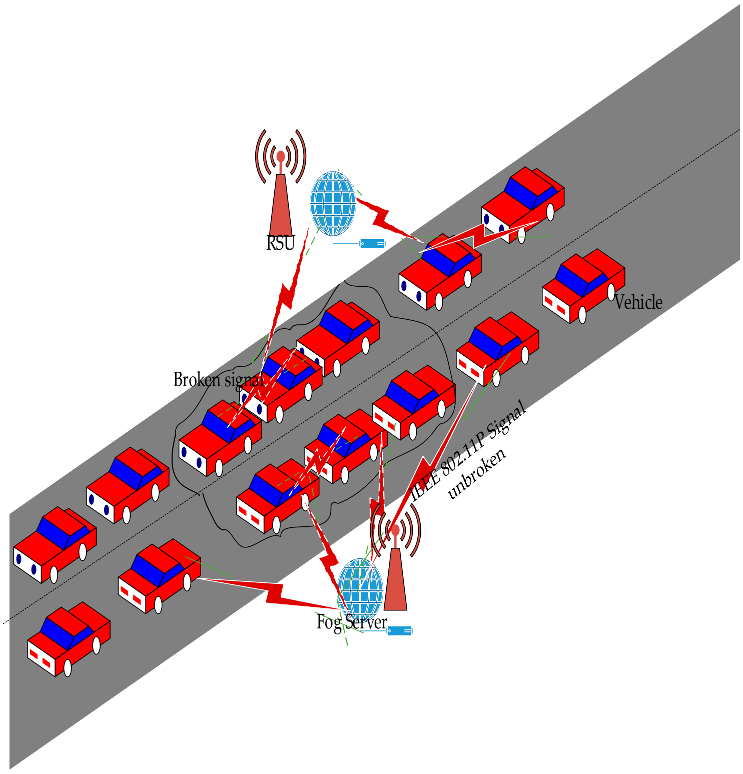


**Figure 3.** Vehicular communication channel DoS Jamming Signal Attack Model (D-JSAM).

## 4. Prevention Mechanisms of the Proposed Scheme

### *4.1. Proposed Scheme System Architecture Model (PSAM)*

In this research, PSAM represents the proposed scheme system architecture model. It is used for the detection of end-to-end delayed path packets of vehicles in the network that have also encountered HDSA attacks with the HDAM. PSAM utilizes the attacked packet detection algorithms (APDA) deployed in the PSAM, as shown in Figure 4. The APDA is utilized to capture all forms of attacks categories, including HDSA and all other forms of associated attacks with VANET, as identified with the PSAM. The HDSA categories include PD/FI, DoS JSA, and RCRCO, which would require high memory computation and high bandwidth. Figure 4 depicts the PSAM of this research, whereby the APDA method has been implemented. The APDA method used is attached through every RSU and the FS via a packet detection mechanism that distinguishes exact message positions on the path of the vehicle. It also utilizes ESA communication range (ESACR), which has the objective of evaluating end-to-end delay and jitter experienced in the network.

In addition, one of RSU's main job functions include serving as a gateway for the PSAM for all vehicle communication. The RSU also coordinates with FS to disseminate secure transmissions of V2V communication. The RSU is also connected with the FS logically through wireless or wired means. After the detection of vehicle position, the information or messages are derived based upon the effectiveness of the utilization of the above two attacks models, which include the DoS attack model (DAM) and jamming attack model (DJSAM). These two models (DAM and DJSAM) are together known as the HDSA model (HDAM). These attack models are deployed for the proposed scheme for detection of the HDSA and other attacks, discussed previously in Section 3. HDAM models, as depicted in Figures 2 and 3, utilize RSUs and the FS to process the communication. Thus, HDAM utilizes the IEEE 802.11p beacons and signals for vehicle communication. IEEE 802.11p beacons employ the devices in the VANET, which have on-board units (OBUs) and Tamper Proof Devices (TPDs). These are used to store the comprehensive information for the vehicles, such as position, speed, etc. The position of the vehicles is identified by the velocity of the vehicles, frequency of the vehicles, the vehicle position, and the number of packets sent to the vehicles. The vehicle position identification utilizes the following communication processes: vehicle-to-vehicle (V2V) communication, the vehicle-to-road-side unit (V2RSU), and the inter-roadside-communication unit (RSU2RSU), as shown in Figure 4. The communication process also encompass the relay of IEEE 802.11p beacons that utilize hybrid multicast/broadcast and unicast data transmission. The communication process also sensitizes awareness for road safety and driver vigilance.

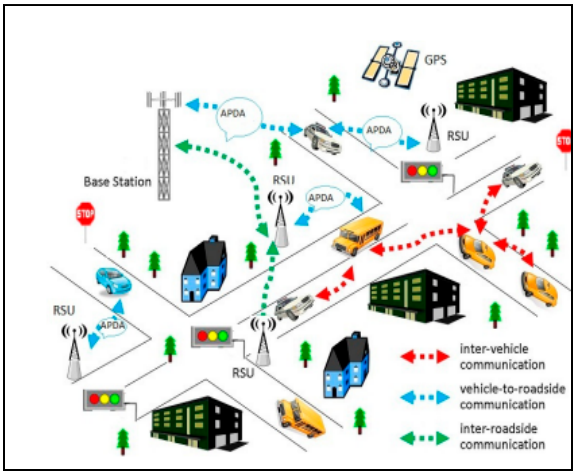

GPS
APDA
APDA
RSU
STOP
Base Station
RSU
APDA
STOP
RSU
APDA
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

**Figure 4.** Proposed system architecture model (PSAM) for the proposed scheme.

In the PSAM, when the packet is not attacked, then the V2V communication, V2RSU, RSU2V, and RSU2RSU communication will not track the path in end-to-end delay of the exact vehicle. This capability includes the tendency to reduce communication overhead (CO) in the PSAM. An algorithm has been designed on the basis of requirements as per the variations in the positions of vehicles in the VANET. The identification of the attacked packets can be done by *V* (velocity) and *F* (Frequency); $\lambda$ is a co-efficient that has been determined by the characteristics of the road and Vmax is the maximum Speed, m as shown in the Equation (1):

$$F = \lambda^* \left| V - \frac{v_{max}}{2} \right| \tag{1}$$

where *F* is the number of packets unicast and multicast (or broadcast) per second. The identification of the attacked packets is done with the below conditions:

The ranges of *F* and *V* are high, as the vehicle's position varies instantly.

The ranges of *F* and *V* are low, as the vehicle's position does not vary instantly.

The algorithm is based upon the variation in frequency, position, and velocity. Algorithm 1 is used for the detection of attacked packets.

**Algorithm 1.** Detection of all attacked packets based on hybrid DoS attacks (HDSA) and other attacked packets in the HDSA model (HDAM).

```
function RECOGNIZE (attacked packet for HDSA in the models).
Start
Discover $F = \lambda^* \left| V - \frac{v_{max}}{2} \right|$
If ($F \geq$ high && $V \geq$ high) then
  recognize (Attacked packet)
set attacked packet detection Alg (req) then
    Start when validated (request)
return true
else
  if ($F \leq$ low && $V \leq$ low) then
    return invalid request
else
  set attacked packet detection Alg (req)
    end if
   end if
  end
end
```

The above algorithm can be applied prior to the verification time and to increase the security. The algorithm is utilized for detection of unacceptable requests with the attacked packet. It can also be utilized to avoid the end-to-end delay CO on the path of vehicles in the network. It is also worth noting that establishment of a safe and secure root is another matter, and sending the data in secure manner is also another matter. Even if the roots are safe, they cannot be 100% trusted. The proposed scheme model utilizes a Vehicular RSA algorithm (VRA) type at the transmitter end. The transmitting node also shares a key to the universal port (a port that keeps an eye on data sharing and vehicle information), which is established at the center of the network. The receiving node has the same key, which is shared by the transmitting node, but obviously there must be an intermediator who can verify it. The central port plays the role of the intermediator. The receiving node and the transmitting node both send their key with the added registration number of the vehicle to the central port. Suppose the key is 6612 and the registration number of the transmitter is 31, then the shared key will be 6612 + 31 = 6643. The receiver will also show 6612, and assuming that the registration number of the receiver is 45, then the key which is shared by the receiver will be 6612 + 45 = 6657. The central port subtracts the registration number from both the sender and transmitter shared value. If after the subtraction both share the same common key, the decryption key is shared by the central port.

The vehicular RSA encryption algorithm used at the transmitter end to further secure the network given as Algorithm 2.

**Algorithm 2.** Vehicular RSA Encryption Algorithm.

```
if Sender vehicle $S_v$ creates a key then
    receiver vehicle $R_v$ and $S_v$ creates two large prime numbers ($P$ and $Q$) then//note that $P$ and $Q$ are each about same number of digits long, and are selected such that their product is long
  set $S_v$ and $R_v$ to determine the value of large number $N$ using, $N = PQ$ then
                    $R_v$ and $S_v$ Creates the value $M$//using the given expression below, Euclidean algorithm
    $M$ = phi ($N$) = ($P$ – 1) ($Q$ – 1)
    if $S_v$ and $R_v$ select any integer value $E$ then
    $E$ = positive integer//$E$ lies between, $0 < E < M$
    function GCD ($M$, $E$) = 1//(GCD is Greater Common Divisor)
input: $S_v$ and $R_v$ calculate the value of $D$
Output: The quotient and remainder of $M$ and $E$
If ($E \times D$) = 1 (mod $M$) then
($E \times D$) mod $M$ = 1 &
    if $S_v$ and $R_v$ create the Public key: $E$, $N$ then
    set $S_v$ and $R_v$ to create Private Key using $D$ and $N$
Encryption/Verification:
    if $S_v$ and $R_v$ can utilize original plain text (a block value) = $X$ ... $X < N$ then
    $S_v$ and $R_v$ obtain Ciphertext = $C$ ... $C = (X^E) \bmod N$
end if
    Decryption/Signing:
    if $S_v$ and $R_v$ Utilize Ciphertext = C then
    $S_v$ and $R_v$ utilizes Deciphertext = Y
    end if
    end if
    end if
    end if
    end
```

The proposed vehicular RSA is an algorithm used by modern fog computing and cloud-based techniques to encrypt and decrypt packet data during the data transmission. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography because one of the keys can be given to everyone. The other key must be kept private.

Figure 5 represents the authentication process of data packets using the vehicular RSA encryption algorithm. The transmission of data packets from the transmitting vehicle or node to the receiving vehicle or node is represented by an arrow. Every vehicle in VANET comprises an individual private key generated by each node along with the public key. The public key is same for every node, whereas the private key is different. Therefore, whenever a node wants to transmit the data, a private key along with the public key must be generated and transmitted along with the packet. In the case where the key is matched, it means that the node is genuine and the transmitting node transmits the data, otherwise the node is considered an attacker node and the route is changed without forwarding data to the attacker node.

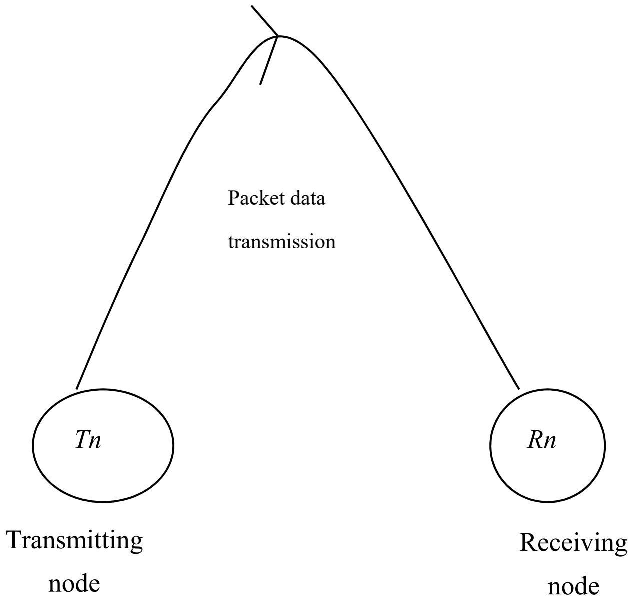


**Figure 5.** Authentication of data packets using vehicular RSA encryption algorithm.

The process of authentication of data packets in the proposed scheme models are also required to be extended for further investigation on storage of data in a model, based upon the ESA, which is determined based upon the DJSAM elliptical segment transmission range. This is due to the fact that there is high anticipation of HDSA that can be identified in the ESA that would require further investigation within a specified transmission range in VANET. In addition, Vehicular Fog Computing and Cloud-based (VFC) integration, which utilize ESA, are important in the network design. These are used to solve any limitations in storage and efficient computation in VANET. VFC should also be deployed in the elliptical segment area transmission range (ESATR) in order to also investigate trustworthiness, using the storage prevention mechanism in the proposed scheme network, which will be investigated subsequently.

### *4.2. Fog Computing (FC) Storage Preventive Model*

VANET is mainly designed to optimize the communication network between the vehicles. Due to the high movement of the vehicles, Fog Computing and cloud integration (VFC) has gained attention in this area. Fog Computing that denotes VFC can store a lot of data, which can be reused and can be aggregated to prevent time succession searches, as the vehicles have a lot of on-board storage [37].

Broadcasting data for vehicles in the network differ, based upon fog computing status. When the vehicle status is in the state of being elected for communication, in which the vehicles discover the decision of subsequent state on vehicle location information and speed, broadcasting of vehicles data packets ($d_p$) are considered so that they arrive at CM (Cloud member) within the network. When the CL (Cloud leader) produces data packets, it confirms through the information acquired from vehicles if packets are either received effectively or not. When the vehicles in the cloud have the data packets, then vehicles verify the packet source. When the source is from the parent cloud, they multicast the data packet to the cloud member, otherwise, the packet is taken from the vehicle as the state election mode.

Later, vehicles unicast the received packets towards the parent cloud to send the packet until packets arrive at the cloud leader, which discloses the vehicle information. Accordingly, as shown in the below algorithms, if the cloud leader produces a data packet, initially it verifies the packet source. When the data packet approaches from enode-B (an element of the long term evolution (LTE) radio access network), the cloud leader transfers the data packet to each cloud member or the packet is sent from the parent cloud ($pr_c$) member. In this circumstance, the cloud leader sends the data packet to the cloud member and generates the LTE data packet ($LTE_{dp}$), which transfer the packets to enode-B with the novel original received packet from the vehicle. In the end, the packets are updated as cloud leader vehicle information (CLvInf).

The PSAM utilizes the multicast/broadcast and unicast modelling in order to fulfill the requirement as needed. Obviously, the multicast architecture incurs some latency and as it broadcasts the data, it will consume some time.

Algorithms 3, 4, and 5 decrease the issues of the broadcasting storm within the network by lessening the iterated data broadcasting and by keeping less overhead information. They also broadcast the specific data using appropriate vehicles or nodes that also decrease the network load. The reduction of network load action taken is necessary due to consideration of overwhelming messages that may occur as a result of all forms of attacks, including HDSA and DoS JSA in the network. They also lessen the problem of network disconnection by lessening the regular downloading and subscription to the network [38]. Table 1 depicts the notation and descriptions of the algorithms and the models terms.

**Algorithm 3.** IEEE 802.11p-LTE CM.

```
On $d_p$ generating or receiving: //on receiving or generating the data packets
  filter $Id_{data}$ or $req_{data}$; //Filter on Packets
If ($Id_{data}$, $req_{data}$) ϵ CLvInf &
If $d_p$ is from $pr_c$ then
multicast on $d_p$ to CM; //Multicast situation
else
  unicast $d_p$ to $pr_c$ CL //Unicast situation
Update vInf;
  end if
end if
end
```

**Algorithm 4.** IEEE 802.11p-LTE Cloud leader (CL).

```
for on $d_p$ generating or receiving then
filter $Id_{data}$ & $req_{data}$;
If ($Id_{data}$, $req_{data}$) ϵ CLvInf &
If (On $d_p$ is from eNodeB) then
    send on $d_p$ to CM;
  else
  broadcast $d_p$ to CM
develop $LTE_{dp}$ and send to eNodeB then
   Update vInf;
  end if
end if
end for
end
```

**Algorithm 5.** IEEE 802.11p-LTE eNodeB.

```
for $d_p$ generating or receiving;
filter $Id_{data}$ and req_data;
if ($Id_{data}$, $req_{data}$) $\epsilon$ (CL, vInf) then
broadcast $LTE_{dp}$ to eNodeB-fog then
broadcast $LTE_{dp}$ to CL then
send to server-fog then
broadcast $LTE_{dp}$ to eNodeB then
broadcast $LTE_{dp}$ to CL
Update eNodeB;
end for
end if
end
```

**Table 1.** Notations and descriptions utilized in the algorithms and models.

| Notations | Descriptions |
|---|---|
| $d_p$ | Data packet |
| CM | Cloud member |
| LTE | Long term evolution |
| CL | Cloud leader |
| $pr_c$ | Parent cloud |
| enode-B | Element of LTE network |
| LTE_Datapacket | LTE Data packet |
| T | Time of transmission |
| Rv | Receiving vehicle |
| Sv | Sending vehicle |
| (rv&ap) | Receiver with access point |
| (ap&s) | Access point and server |
| (s&frv) | Server with feedback reporting from vehicle |
| t(p) | Server processing time |
| CLvInf | Cloud leader vehicle information |
| $LTE_{Datapacket}$ | LTE data packet |
| $Id_{data}$ | Identified data packet |
| $req_{data}$ | Requested data packet |
| VInf | Vehicle information |
| VANET | Vehicular ad hoc network |
| VCC/VCF | Vehicular cloud computing/Fog computing |
| SUMO | Simulation of urban mobility |
| SDN | Software define network |
| FCM | Fuzzy-c mean |
| IoE | Internet of everything |
| MGA | Modelling to generate alternative |
| V | Velocity |
| F | Frequency |
| $\lambda$ | Road characteristic coefficient |
| Vmax | Maximum speed |
| ROI | Region of interest |
| Alg(r) | Algorithm request |
| FFBPNN/GA | Feed forward back propagation neural network utilizing genetic algorithm |
| DoS | Denial of service |
| AKA | Authentication and key agreement |

In order to investigate HDSA and DoS JSA, including other attacks, using the PESATRM model, the fog server (FS) and fog level (FL) authentication preventive mechanism is important, which should be utilized in the Elliptical Segment Area Transmission Range Model (ESATRM), as explained below.

### *4.3. Elliptical Segment Area Transmission Range and Authentication Prevention Model*

In order for vehicles to communicate effectively and get authenticated, a specified transmission range of vehicles, which also utilize HDAM, is designated in the network. The designated transmission range is based upon the elliptical segment area (ESA) transmission range (ESATR), which utilizes V2V standardized road safety information exchange (SRSIE). The ESATR requirement is also based upon a model adoption in VANET. Based upon the model, the contribution of HDAM is also important for investigation. The model requires a further authentication prevention mechanism in the network. Therefore, this research investigates a model in VANET known as the proposed scheme elliptical segment transmission range model (PESATRM). PESATRM includes the tendency to utilize a secure authentication prevention method, which is integrated in the VANET communication process design. This is also used to mitigate all forms of attacks, including HDSA and DoS JSA attacks. Further secure authentication in the PESATRM can be achieved through FS and RSU deployment. In the PESATRM, the V2V communication process utilizes IEEE 802.11p beacon transmission to communicate and also secure the network links. This provides the capability for each vehicle to exchange messages securely within a specified ESATR. Based upon this, vehicles move along in the same direction of travel to their intended destination (as shown in Figure 6). Therefore, the PESATRM has been developed from a modified circular segment area model (CSAM) adopted in a previous study [39].

However, investigation revealed that the CSAM is insecure based upon limitations in HDSA and DoS JSA and other forms of attack investigation. In addition, another limitation worth noting is that the CSAM design does not utilize fog computing and cloud-based (VFC) integration investigation. Therefore, it is suggested that the PESATRM communication process should be designed to include VFC employing authentication/KDE (AKDE) to further secure the network. In addition, it is estimated that designing a secure PESATRM would also prevent high incidences of communication overhead (CO). CSAM limitations also include increased communication overhead (CO).

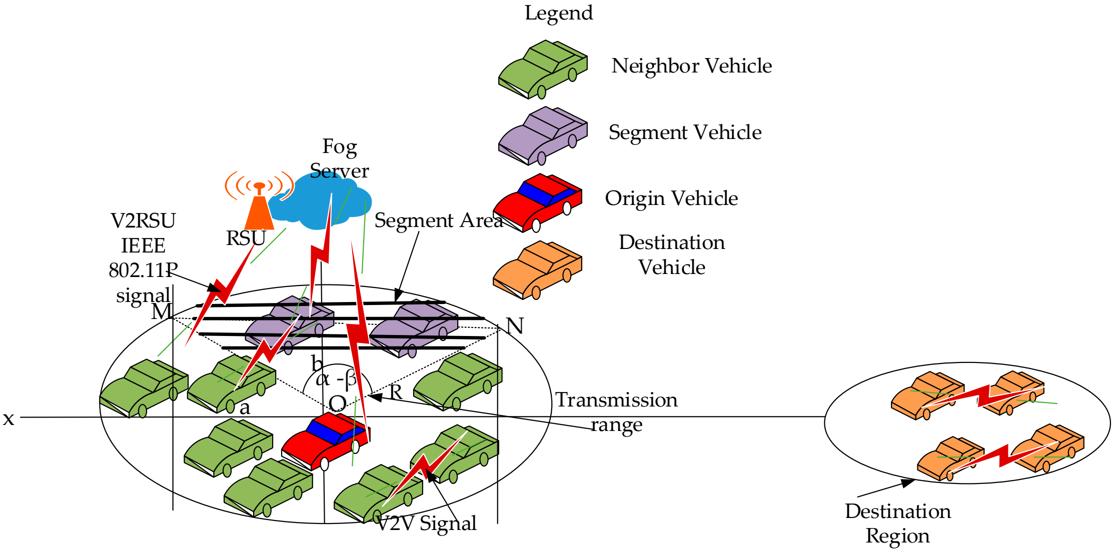


**Figure 6.** Vehicles in the Elliptical Segment Transmission Range Model (ESATRM).

In the design of PESATRM, we require that integration with the PSAM model is possible, which should include VFC. VFC integration provides enhancement in the end-to-end delayed path attacked packet detection process. This is based upon the fact that the neighbor-vehicle-to-neighbor-vehicle (NV2NV) communication process requires further AKDE. Moreover, the SRSIE process that prevents

CO due to the end-to-end delay/jitter path in vehicles is anticipated in the network, which requires trustworthiness. Secure VFC and FS integration provide secure real-time detection of all other forms of attacks, including HDSA and DoS JSA, which utilize the IEEE 802.11p beacon transmission relay process in a specified ESATR.

Furthermore, in the design of the PESATRM, rapid topology changes in VANET are important for investigation. This is because HDSAs, including DoS JSA and other vulnerabilities, are eminent in the air, or in the open environment in which VANET deployment occur. Therefore, the PESATRM is also designed to detect traffic in DoS JSA and its associated vulnerabilities faster and more accurately. The network topology design should utilize VFC and AKDE, which are able to store large volumes of data utilized for secure delivery of SRSIE. Based upon this provision, it is possible for the proposed scheme to detect and mitigate HDSA, including DoS JSA and associated vulnerabilities that would incur CO in the network. In addition, VFC provides increased space search for SRSIE in the network and requires hybrid optimization algorithms (HOA).

HOA deployment and integration in VANET is important. It provides swarm intelligence and utilizes a heuristic approach in solving VFC limitations. Based upon this, we require that integration of PSAM and PESATRM models should include intelligence for efficient ESATR. HOA integration with VFC utilizes HOA heuristics to solve problems in the network, such as end-to-end delay and jitter performance evaluation. Based upon this, the dynamic transmission range is provided in the network. Dynamic transmission is usually more effective in maintaining connectivity. HDSAs, including DoS JSA and all other forms of DoS attacks, can be detected and eliminated from the network when a specified ESATR is deployed in the PSAM and the PESATRM integration. We also anticipate that the design of ESATR needs to be more secure. Comparatively, the circle segment transmission range (CSAM) that PESATRM was modified from is more confined. Therefore, we anticipate that the CSAM will incur a lot of trustworthiness concerns, since it does not detect and eliminate HDSA and its associated DoS JSA in the proposed scheme models. Figure 6 is used to explain the deployment of the PESATRM. It is anticipated logically for the PESATRM to utilize AKDE.

In Figure 6 (as shown below), the vehicles within the ESATR are also known as neighbors. These neighbor vehicles (NV) are secure in the network using the AKDE method. NVs are also required to keep one global key (Gk). The Gk provides the requirement in authentication of the NVs in the models (PSAM the PESATRM). The method of acquiring the Gk, which also represents the public key, is given through FS and the RSU. In addition, secure sharing of the Gk is important. This must be complied with for every NV using NV2NV communication. In addition, secure sharing of the Gk includes SRSIE accurately. Therefore, implementing a further authentication mechanism is required in the network, which is also investigated in the models. In addition, the objective of the NV2NV communication is to utilize authentication of each NV in the PESATRM. This verifies that the communicating NV entities are all neighbors with each other. Subsequently, NVs exchange "hello" messages to initiate the communication process. Thus, NVs are capable of utilizing sufficient time in the NV2NV communication to be able to transmit SRSIE. This successfully leads to processing of standardized road safety traffic emergency information (SRSIE) exchange for VANET in the same ESATR.

Based upon this, Figure 6 also depicts the PESATRM, which utilizes V2Vcommunication. The PESATRM NVs exchange "hello" neighbor messages. The hello message exchanged by NVs is initially broadcast or multicast and finally unicast using NV2NV and secure NV communication. NV2NV and secure NV communication processes include neighbor vehicles (NV), origin vehicles (OV), and the destination vehicle (DV). Each NV that communicates with other NVs initially gets authenticated. Afterwards, NVs transfer the Gk securely with each other. Subsequently, NVs or NV2NV simultaneously transmit the SRSIE with each NV.

The message transmitted is also used to obtain the direction, speed, and time information of each NV. Since the NV2NV communication process includes secure sharing of the common Gk and SRSIE, these are designated to occur in the proposed ESA. Each NV segment S is as shown in Figure 6 with the dark black lines. The probability analysis of the proposed scheme PESATRM will be determined subsequently below. For now it is important to determine the ESATR as follows:

From Figure 6, the area of the ellipse is $A = \frac{b}{a}\pi a^2 = \pi ab$.

An elliptic sector is the region bounded by an arc and line segments connecting the center of the ellipse (which is the origin in the figure) and the arc endpoints.

To determine the elliptic segment area, we let lines $x = acos \propto$ and $x = acos\beta$ be perpendicular to the $x - axis$. The coordinates of M and N are $(acos \propto,\ bsin \propto)$ and $(acos\beta,\ bsin\beta)$, respectively. Therefore, the area of the elliptic sector $MON$ is determined as:

Segment area

$$S_{Area} = [MON] = \frac{b}{a}\left(\frac{\propto -\beta}{2\pi}\right)\pi a^2 = \frac{1}{2}(\propto -\beta)ab.(\alpha > \beta) \quad (2)$$

An elliptic segment area is bounded by an arc and the chord that connect the arc's endpoint.

Hence, the elliptic segment area is given in Equation (3) as:

$$S_{Area} = [MON] = \frac{ab}{2}(\propto -\beta) - \frac{b}{a}(\frac{a^2}{2}\sin(\propto -\beta)) = \frac{ab}{2}((\propto -\beta) - \sin(\alpha - \beta)) \quad (3)$$

Figure 6 also demonstrates the movement of vehicles in the designated PESATRM. The PESATRM utilizes maximum transmission range. It is based upon specified NV relationships with each other NV. Based upon this, each NV is required to transmit the IEEE 802.11p beacon's "hello" message with every other NV. The NVs also obtain their speed, location, direction, and time information. At the same time, further AKDE is required in NV2NV communication. AKDE is initiated against all forms of attacks, including HDSAs, such as DoS JSA attack, which occur at different speeds, directions, and times. It is also achieved through the FS and the RSU data transmission and authentication process based upon each NV, OV, and DV (NODV) communication process, as follows.

### *4.4. Fog Server (FS) Further Authentication Process in the Elliptical Segment Area*

The models encompass PSAM and PESATRM. These models utilize FS and RSU for further authentication processes. This is in order to ensure safe arrival of NODVs that travel in the same ESA. The authentication process involves two-fold performances. In the first performance, V2V communications are authenticated with every other NODV. In addition, they also share the common Gk securely. Based upon this, each NODV is capable of securely acquiring the Gk by FS and the RSU. The authentication (AKDE) and secure SRSIE of NODV ensures that all vehicles that fall in the same ESATR have achieved further trustworthiness protection in the network. Based upon the PESATRM model, we also assume that the use of Vehicular RSA (VRSA) public key deployment is important. This include utilizing the common Gk as each NODV public key.

Each NODV vehicle or node is also required to pass a VRSA authentication process check (this was formally achieved previously through the PSAM). The following further authentication preventive mechanism, which also utilizes the Gk, is formally deployed in the FS and the RSU authentication process, as follows. This also utilizes the following assumptions that are important for the FS and RSU further authentication process of the PESARTM integration with PSAM models, as follows:

- FS and RSU message authentication denotes VANET safety message announcement as standardized.
- PSAM integration with the PESATRM utilizes the FS parameters, which include $G_k$, $C$, and $T$, where $G_k$ is the global public key of the sender vehicle or NODV, $C$ is $Cert_{Xn}$ ($n$ denotes possible pseudonyms of vehicles of entity $X$, whereby one is also a pseudonym of NODV and others are collected pseudonyms of other NVs), and $T$ denotes the authentication tag, which includes the integration of PSAM and PESATRM, which is installed through RSU and the FS.

- Based upon each possible signer vehicle that occurs in the PESATRM, a validation $\sigma_X$ is important. Here, $\sigma_X$ denotes the PESATRM signature (PESATRMS) created by vehicle entity $X$. When a vehicle entity $Y$ is authenticated by a symmetric encryption with key $G_k = K$, it is written as:

$$E_{Gk}(Y)$$

The FS and RSU further authentication algorithm is given as Algorithm 6.

**Algorithm 6.** Fog Server Further Authentication Algorithms for Proposed Models.

```
1.  if Neighbour vehicle $A$ (NVA) sends authenticated safety message (ASM) and shares $Gk$ through an initial broadcast/multicast and finally unicast to all vehicles within same ESATR, based upon the advocated scheme then
2.  Assume neighbour Vehicle $B$ (NVB) is in the same ESATR that also represents the next single hop vehicle (NSHV), which also utilizes this application and receives the ASM from $NVA$ &
A.  if $NVB$ = NSHV then
B.  generates a random key $K$ and computes the proposed PSAM and the PESATRM parameters $G_k, C, T$;
C.  creates the PESATRMS $\sigma_{NVB}$ over the calculated PSAM and PESATRM parameters through its current application-specific pseudonym, including $n-1$ collected pseudonym, then
D.  Set $NVB$ to encrypt PESATRMS with the chosen key K then
E.  send resulting ciphertext through the PSAM and PESATRM parameters;
3.  if $NVB \rightarrow NVB\colon\ G_k, C, T$ then
4.  set $E_{Gk}(Cert_{NVB1}, \ldots, Cert_{NVBn}, x_{NVB1}, \ldots, x_{NVBn}, \sigma_{NVA})$
5.  If NV$A$ $\rightarrow$ NV$B$ then
6.  set $E_{Gk}\big(Cert_{NVA1}, \ldots, Cert_{NVAn}, x_{NVA1}, \ldots, x_{NVAn}, \sigma_{NVB}\big)$
7.  end if
8.  end if
9.  end if
10. end
```

In the second performance, further FS and RSU authentication processes are employed. Each V2V communication process utilizes and transmits IEEE 802.11p beacons for SRSIE. This takes place so that each NODV can also share and utilize SRSIE amongst themselves. This performance process employ probability analysis, including encryption/AKDE of each NV communication, followed by successful data exchange in the ESATR.

VANET application models, such as the PSAM and PESATRM integration, require an exchange of application-specific trustworthiness data, which utilizes the secure *Gk* sharing. Thus, the data exchanges must first ensure that they have been protected from any form of HDSA, including DoS JSA of NODV, which does not use the application. This enables each communicating NODV that falls in the same transmission range to become convinced that each vehicle is eligible to securely obtain the *Gk*. Moreover, vehicles also become securely authenticated and are capable of exchanging SRSIE with each other accurately [40].

The probability analysis that encompass the PSAM and the PESATRM integration for finding each NSHV also utilizes the proposed scheme FS and RSU authentication algorithm for exchange of SRSIE. This occurs in the encrypted non-shadowing environment (ENSE) region, as determined below.

### *4.5. Probability Analysis of Vehicles Based on Elliptical Segment Area Transmission Range*

This section discusses the probability analysis of vehicles based upon PESATRM. The section also includes utilization of the NSHV concept of authentication based upon the FS and the RSU authentication algorithm, and secure SRSIE. Based upon this, NSHV links are set up to forward the attacked detected packet, utilizing the transmission and relay of IEEE 802.11p beacons in the ESATRM. This is based upon the communication process of NV-to-NV utilized in the network. Based upon this, a sender $NV_A$ is required to find at least the NSHV $NV_B$ that is in the same ESATR. This is followed by authentication and subsequent transmission of the SRSIE, which is based upon the PESATRM deployment. NV/NODV that are present in the ESATRM utilize three parameters, namely density $\lambda$, segment angle $(\alpha - \beta)$, and transmission range $R$. The PESATRM probability analysis has an objective of analyzing the impact of the parameters, $(\alpha - \beta)$, and $R$. In addition, the PESATRM is also anticipated for use where it is also important for providing secure authentication. This secures each NV2NV communication, and also sharing of *Gk* with individual NVs. The objective of utilizing sharing of *Gk*s that fall in the same ESATR also include the probability analysis of locating at least one NV for sharing of *Gk*s in the segment area. This objective can be achieved when different values are assigned to $(\alpha - \beta)$ in increasing order, until a NODV is found in the ESATR that would authenticate and also share the common *Gk* with every other neighbor vehicle during the vehicle movement of NODV in the ESATR.

The movement of NODV is considered to take place using a two-dimensional network area. This is based upon the ESATR. NODV availability in the network follows a Poisson distribution with NODV density $\lambda$. When considering the mean density of NODV in the network, the number of NVs that are present in the ESATR is obtained using a Poisson distribution. In addition, each NODV arrival also depends on how successfully it is able to initially be authenticated with each other NV. It is then followed with the secure sharing of the *Gk* with every other NODV vehicle. This also includes exchange of the standardized safety and road emergency conditions with each driver or vehicle on the road.

The proposed scheme uses NODV position to initially broadcast/multicast and finally unicast information to other NVs that fall in the same ESATR. In addition, it is presumed that the proposed scheme PESATRM probability analysis also utilizes the attacked packet detection algorithm (APDA) that was achieved in the PSAM. This is in order to mitigate against HDSAs, including DoS JSA attacks, which may be encountered in the ESATR. The proposed scheme PSAM, which is already integrated with the PESATRM, is also deployed together to prevent malicious nodes becoming part of the network. The NODV position information is represented through both $x$ and $y$ coordinates on a plane using a 2D network model.

Optimal transmission range investigation for VANET has been conducted by various researchers in [41,42]. In those studies, it was revealed that transmission range requirements in VANET decrease with increases in vehicle density. High density vehicular traffic situations require a smaller transmission range. Moreover, we recall that NV2NV communication would also require authentication and encryption of data, including the sharing of the *Gk* in a non-shadow environment (ENSE). The ENSE avoids real-time conflict in transmissions of data authentication and exchange of information in the shadow area. Based upon this, neighbor vehicle transmissions would result in collision and congestion [43]. Therefore, we adopt our previous proposed scheme, the ESATR detection process for DoS attacks [44]. By referring to the efficient transmission range for NV, we chose a transmission range between 250 and 550 m. However, we consider the smaller transmission range of 250 m as effective. This is because of reduced CO, which can be utilized in the elliptical segment probability analysis of the NV/NODV.

We consider $X$ as the random variable, which represents the number of NV/NODV present and located in the ESATR, whereby each NV/NODV possesses the global key (*Gk*). After each NV/NODV is authenticated and shares the *Gk* securely, the probability $P^{ENSE}_{S_{area}}(X = n)$ in the presence of $n$ NV/NODV in the proposed ESATR, which utilizes encrypted SRSIE, in non-shadow environment (ENSE) can be obtained in the given Equation (4) as:

$$P^{ENSE}_{S_{area}}(X = n) = \frac{(\lambda \times S_{area})^n \times e^{-(\lambda \times S_{area})}}{n!} \tag{4}$$

Substituting the value of $S_{area}$ from Equation (3), we obtain Equation (4) as:

$$P_{S_{area}}^{ENSE}(X=n)=\left[\frac{\left[\lambda\left\{\left(\frac{ab}{2}(\propto-\beta)-\frac{b}{a}\left(\frac{a^2}{2}\sin(\propto-\beta)\right)=\frac{ab}{2}((\propto-\beta)-\sin(\alpha-\beta))\right\}\right]^n}{n!}\right. \\ \left.\times e^{-\lambda\{(\frac{ab}{2}(\propto-\beta)-\frac{b}{a}(\frac{a^2}{2}\sin(\propto-\beta))=\frac{ab}{2}((\propto-\beta)-\sin(\alpha-\beta))\}}\right] \tag{5}$$

$$P_{S_{area}}^{ENSE}(X=0)=\left[\frac{\left[\lambda\left\{\left(\frac{ab}{2}(\propto-\beta)-\frac{b}{a}\left(\frac{a^2}{2}\sin(\propto-\beta)\right)=\frac{ab}{2}((\propto-\beta)-\sin(\alpha-\beta))\right\}\right]^0}{0!}\right. \\ \left.\times e^{-\lambda\{(\frac{ab}{2}(\propto-\beta)-\frac{b}{a}(\frac{a^2}{2}\sin(\propto-\beta))=\frac{ab}{2}((\propto-\beta)-\sin(\alpha-\beta))\}}\right]$$

$$P_{S_{area}}^{ENSE}(X=0)=e^{-\lambda\{(\frac{ab}{2}(\propto-\beta)-\frac{b}{a}(\frac{a^2}{2}\sin(\propto-\beta))=\frac{ab}{2}((\propto-\beta)-\sin(\alpha-\beta))\}} \tag{6}$$

The probability of $P_{S_{area}}^{ENSE}(X \geq 1)$ in the presence of at least one vehicle in the segment area with encryptin and authentication and sharing of global key *Gk* in a non-shadowing environment can be expressed as given in Equation (7):

$$P_{S_{area}}^{ENSE}(X \geq 1)=1-e^{-\lambda\{(\frac{ab}{2}(\propto-\beta)-\frac{b}{a}(\frac{a^2}{2}\sin(\propto-\beta))=\frac{ab}{2}((\propto-\beta)-\sin(\alpha-\beta))\}} \tag{7}$$

The above PESATRM probability analysis model, which is integrated with the PSAM, is proposed in addition to the message broadcast algorithms that were investigated. These have been used to decrease the broadcasting storm in the network. Moreover, the models' integration reduces trustworthiness concerns in the network. The combined effect of the PESATRM and algorithms also increase established trust in the network. This was possible through achieving an efficient ESATR. In addition, the algorithms implemented in the proposed scheme models PESATRM and PSAM also lessen the iterated broadcasting to keep less overhead information and decrease the network load.

The process of using the PESATRM and PSAM integration probability models and the broadcast/multicast and unicast algorithms to verify the network is secured from HDSAs, including DoS JSA and other associated attacks. Even though the deployment of these models in the scheme were satisfactory, in order to make the model more efficient for selection of trustworthy vehicles or nodes in the network, the Cuckoo/CSA (ABC) optimization algorithm, which include swarm intelligence, is applied to select more trustworthy nodes. This is based upon the probability of legitimate selection of the nodes to be part of the network. Therefore, probability analysis specification selection using Cuckoo/CSA (ABC) for selecting the legitimate nodes to be part of the network communication process is determined as follows. Table 2 shows the Cuckoo/CSA (ABC) specification.

**Table 2.** Cuckoo/CSA (ABC) specification.

| CSA Population | Fitness Parameters Feedback |
|---|---|
| Total number of vehicular nodes in the coverage elliptical segment region | Probability of new vehicles as part of the network, $\boldsymbol{V_i^k}$ fitness value |

To determine

$$\text{Fitness value} = \boldsymbol{V_i^k} \tag{8}$$

where $\boldsymbol{V}$ is the vehicular node, $\boldsymbol{k}$ is evolved the from initial point $(\boldsymbol{k}=0)$ to the total gen iteration number, Cuckoo/CSA (ABC) has a powerful feature to generate new candidate vehicle or node solutions to be part of the network. Based upon that approach, a new candidate solution $\boldsymbol{V_i^{k+1}}(\boldsymbol{i} \in [1\ldots,\boldsymbol{N}])$ is produced through disturbing the current $\boldsymbol{V_i^k}$ with a position change $p_i$. $N$ is the number of vehicular nodes in the network. To obtain $\boldsymbol{p_i}$, random step $\boldsymbol{s_i}$ is generated through symmetric Levy distribution using an algorithm from a previous study [45].

Finally, the solution for a new vehicular node solution, $\boldsymbol{V_i^{k+1}}$, is obtained using:

$$\boldsymbol{V_i^{k+1}} = \boldsymbol{V_i^k} + \boldsymbol{p_i} \tag{9}$$

Then, under replacement of nodes a set of individual new nodes that should be part of the network is probabilistically chosen and replaced with malicious or attacker nodes. Each $\boldsymbol{V_i^k}$ $(\boldsymbol{i} \in [1\ldots,\boldsymbol{N}])$ can be chosen with a probability $\boldsymbol{P_a} \in [0,1]$

The operation can be done with the following model:

$$\boldsymbol{V_i^{k+1}} = \begin{cases} \boldsymbol{V_i^k} + \text{rand.}\left(\boldsymbol{V_{r_1}^k} - \boldsymbol{V_{r_2}^k}\right) \text{ with probability } P_a, \\ \boldsymbol{V_i^k} \text{ with probability } (1 - \boldsymbol{P_a}), \end{cases} \tag{10}$$

where rand is a random number normally distributed, and $\boldsymbol{r_1}$ and $\boldsymbol{r_2}$ are random integers from 1 to $\boldsymbol{N}$.

After producing $\boldsymbol{V_i^{k+1}}$ it must be compared with its past value $\boldsymbol{V_i^k}$. If the fitness value of $\boldsymbol{V_i^{k+1}}$ is better than $\boldsymbol{V_i^k}$, then $\boldsymbol{V_i^{k+1}}$ is accepted as the final solution. Otherwise, $\boldsymbol{V_i^k}$ is retained.

The procedure can be done through the following statement:

$$\boldsymbol{V_i^{k+1}} = \begin{cases} \boldsymbol{V_i^{k+1}}, & if\ f\left(\boldsymbol{V_i^{k+1}}\right) < f(\boldsymbol{V_i^k}) \\ \boldsymbol{V_i^k}\ \ , & otherwise. \end{cases} \tag{11}$$

This Cuckoo/CSA (ABC) selection with fitness value $\boldsymbol{V_i^{k+1}}$, as shown in the Equation (11) strategy, demonstrates that only high quality vehicular nodes that utilize relays of high IEEE 802.11p signals (best solution near the optimal value) have the opportunity to interact with the RSU and the FS to deliver emergency feedback information, such as accidents and bad road conditions, to alert road users.

After the selection of the legitimate nodes that are to be part of the network and after routes are discovered, assurance in trustworthiness of the nodes in the network must be maintained, as shown below.

### *4.6. Trust Provision in the Proposed Scheme*

In order to provide trust in the network, it is anticipated that hybrid DoS attacks (HDSA), including DoS JSA and other attacks that may be hard to detect in the proposed scheme models, such as HDAM, PSAM, and PESATRM, have one solution that can also be devised to evaluate the probability information received through a consensus mechanism [46]. Thus, false information reaction due to the HDSAs, including DoS JSA and other attack, would require a vehicle to wait to receive given information based upon binary numbers (ones and zeroes).

Let us consider a vehicle that transmits the information or message, where during the transmission, HDSAs, including DoS JSA and all forms of attacks, occurs because of the neighboring vehicles that disturb or amend the actual information. To secure the network, it is necessary to protect the network from all other forms of external attacks as well. In order to determine the attacks in the network, past information of the transmitting vehicles in the form of binary numbers are considered, on the basis of which the genuine vehicle makes a decision if whether the driver should consider the message as trusted for the vehicle. When the number of zeros is less than ones, the driver would consider the message as the genuine message, or otherwise would ignore the message [47].

$$Vechile_{trust} = \sum number\ of\ ones \tag{12}$$

To decide how instantly the receiving vehicle would trust the vehicle that transmits the message to the base station (RSU and FS), the following equation has been used:

$$t\ (rv) = \sum t(rv\&ap) + t(ap\&S) + t(s\&frv) + t(p) \tag{13}$$

As shown in the above equation, *t (rv)* is the time to choose whether *rv* (receiving vehicle) could trust the *sv* (sending vehicle), *t(rv&ap)* is the time of transmission and reception with the access points and vehicles, *t(ap&S)* is the time of transmission and reception with the access points and server, *t(s&frv)* is the time of transmission and reception with the fog server and feedback of reporting vehicles, and *t(p)* is the server's processing time [48].

In the proposed scheme model, namely PSAM, the communication ranges from 250 to 500 m and the information is transmitted at 30Mbps [49]. Therefore, the transmission time can be determined by using the following equation:

$$\text{Time} = \frac{Distance}{Speed} \tag{14}$$

Distance (d) can be computed by using the following equation:

$$\text{D} = \sqrt{(y_m - y_n)^2 + (x_m - x_n)^2} \tag{15}$$

As shown in the above equation, $(y_m - y_n)$ and $(x_m - x_n)$ show the graph co-ordinates.

### 4.7. RSU Network Prevention Mechanism Against Hybrid DoS Attacks

The network construction is done with the specifications given in Table 3. Algorithm 7 shows the random vehicle positioning (Total Vehicles). Algorithm 8 shows random End-to-end delay detection in Vehicles.

**Table 3.** Network Specifications.

| | |
|---|---|
| Total Number of Vehicles | 60–100 |
| The height of the network | 1000 m |
| The width of the network | 1000 m |
| Node displacement | 150–500 m/s |
| Simulation iterations | 1500 |
| Simulation tool | Matlab |
| Encryption technique | Vehicular rsa |
| mac/phy | IEEE 802.11p |

**Algorithm 7.** Random Vehicle Positioning (Total Vehicles).

```
//for uncertainties in the network, the network is placed in a random position manner
for each n in Nodes/vehicles
    X pos (n) = 1000*rand//creating a random x coordinate
    Y pos (n) = 1000*rand//creating random y coordinate
    Place (Xpos (n), Ypos (n))//Placing the node in their position in the network
 end for
end
```

Function Parameters (Nodes)//this function initializes the node parameters

**Algorithm 8.** Random End-to-end delay detection in Vehicles.

```
for i = 1: Vehicle/Nodes//Loop running for each node
    set End2End Delay_n (i) = Random; //Putting an end-to-end delay value for node acting normal
    End2End Delay (i) = $(End2End\ \text{Dealy}\ \_n)^2$; //now, the expected reality is unpredictable and hence just for the random//architecture is set to be square of the normal delay
 end for
end
```

As the end-to-end delay is initialized, in a similar fashion the other parameters, such as jitter, packet drop, jamming signal resource consumption (RSU/CPU) overutilization, and all other forms of anticipated attacks, including HDSA and DoS JSA attacks, in the network performance metric parameters are also initialized. In VANET, we envisage that there will be no excessive battery consumption. This is due to the fact that as the vehicles that are in the communication process keep moving in order to determine the end-to-end delay of the network, the battery also keeps charging as long as the vehicle are running.

In addition, every node has a different set of parameters. A function is designed to initiate network parameters. The real-time simulation may have a slightly different structure. Networks do not have any fixed structure, nevertheless, for any simulation there are parameters that should be initialized.

### *4.8. Modelling of DoS Threat Prevention*

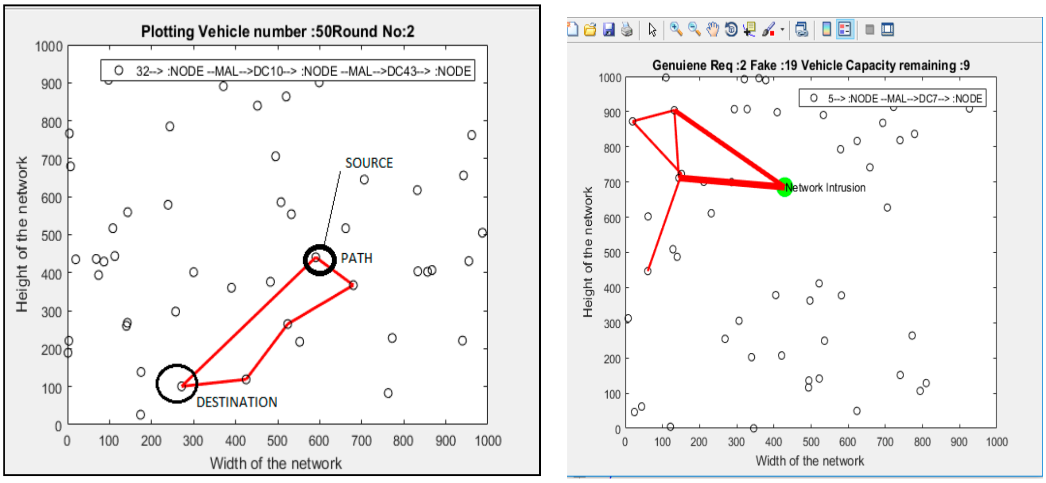
This paper focuses on the prevention of all forms of attacks, including HDSA and DoS JSA attacks. The architecture for the attacks are as follows.

Figure 7a,b represents the path construction and the malicious network for HDSA, including DoS JSA and other attack modes of the attackers, respectively. Figure 7b shows that the intensity of dumping end-to-end delayed packets of the HDSA, including DoS JSA attackers such as jamming of signals, packet drop, and resources consumption via CPU/RSU overutilization, varies at different instances of time. If the intensity of all these forms of hybrid DoS attackers and others are high, obviously the attackers attempt to dump more packets, which results in more packet drop, jamming of signals, and resources consumption via RSU/CPU overutilization, etc., which might affect the RSU for prolonged end-to-end delay in the network. Based upon this, we define the following equation:

$$\text{Tpd} = \text{Pdn} + \text{Pda} \tag{16}$$

Tpd is total packet drop, Pdn is the total number of dropped packets in normal mode, and Pda is the packet dropped when the network is under threat, which has experienced all types of DoS attacks. In addition, we also define the following equation in relation to the types of attacks as:

$$\text{Pdr} = (\text{Tp} - \text{Tpd})/\text{Tp} \tag{17}$$



(**a**) (**b**)

**Figure 7.** (**a**) Path Constructed; (**b**) malicious node HDSA and DoS JSA attackers.

Pdr is packet delivery ratio and Tp is the total number of packets. Due to random behavior of the attacks, the PSAM becomes more sophisticated. Now, the challenge is to identify all the forms of DoS attacks that are experienced in the network. The proposed scheme solution utilizes FFBP-NN and the general functions of FFBP-NN and artificial intelligence are given in Table 4.

**Table 4.** Firely used Feed forward back propagation neural network (FFBP-NN) structure.

| | |
|---|---|
| Total Hidden Layer | 1 |
| Neuron Count | 40 |
| Feeding Iteration | 140 |
| Reverse Iteration | 30–60 |
| PropoFireflytion Type | Linear |
| Algebraic Model | Levenberg |

The artificial intelligence used in the proposed scheme consist of two methods: (1) Training, and (2) Classification/Optimization.

The proposed scheme models, which include HDAM, PSAM, and the PESATRM, utilize two processes in artificial intelligence (AI). They are the training process and the classification/optimization process. In the training process we utilized jitter as the training parameter to train the neural network using the MATLAB neural network tool box. Based upon the training process, a target set is provided as well. The training is orchestrated in two phases. In the initial phase, the training is done for path identification of all vehicles paths that were affected by HDSA, including DoS JSA and other attacks, based upon the communication process experience of vehicles through the transmission of the IEEE 802.11p beacon relay. Then, in the second process, the training is done to identify the vehicles on the route that were also affected by HDSA, including DoS JSA and other attacks. The classification/optimization process optimizes the real-time signal timings during a given attack situation. These would incur HDSAs, including DoS JSA and other attack traffic, which would result in congestion or jamming of signals, packet drop, and resource consumption via RSU overutilization.

Equation (18) below can be defined by the end-to-end jitter based upon AI processes, as follows:

$$\text{Jitr} = \text{E2EDP (at, nt)} + \text{Ntd} \tag{18}$$

From Equation (18), Jitr is the jitter, E2EDP is the end-to-end delay of the path, "at" and "nt" represent advanced (under threat) and normal, respectively. Ntd is the network delay. For each path in every iteration, there will be a jitter. The proposed solution uses the first 450 to 600 iteration data points for training, and then for the next 650 iterations and above to train the structure for identification of the path delayed in the vehicle communication process based upon the proposed scheme and models. Algorithm 9 shows Train_Neural (Reiteration Data, Total Reiterations). The used notations are as follows:

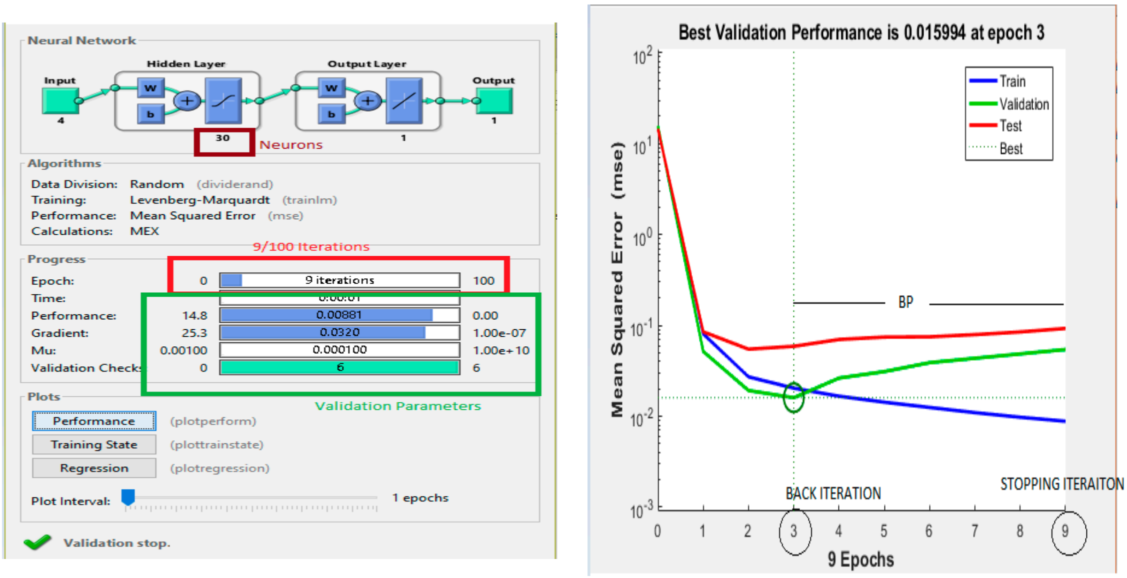
| Notation | Description |
|---|---|
| Tpd | Total packet dropped |
| Pdn | Total dropped packet in normal mode |
| Pda | Packet dropped when network is under threat |
| Pdr | Packet delivery ratio |
| Tp | Total number of packet |
| Jtr | Jitter |
| Dp | Delay path |
| "a" | Advanced (under threat) |
| "n" | Normal (no threat) |
| Nd | Network delay |
| k | Total neurons |
| Avg_jitter | Average jitter |
| Max_jitter | Maximum jitter |
| Min_jitter | Minimum jitter |
| Tdp | Total delivered packet |
| Tm | Total time of packet transfer |

**Algorithm 9.** Train_Neural (Reiteration Data, Total Reiterations).

```
for i = 1: Total_Reiterations
    setTraining_Data (i) =Reiteration_Data (i) then;
    Target_Lable (i) = Path_ID;
end for
NeuralI = Initialize_Neural (Training_Data, Target_Label, k); //k is Total Neurons (40 in proposed case)
NeuralI.TrainParam.Epochs = 140; //total training iterations
Train (NeuralITraining_Data, Target_Label); //training with Initialized Neural and Training data
end
```

The training section leads into the following (Firefly/GA) FFBP-NN structure.

Figure 8a illustrates Feed forward propagation structure and Figure 8b illustrates the back propagation Firefly graph. Based upon the graph, the proposed scheme and the models determine the training data jitter and also validate it. The training data jitter also represents the deviation between predicted y value and also the actual y value, which is the measured MSE (mean square error). In addition, based upon Figure 8b, we can also realize that we have 9 epochs of the proposed scheme model. This implies that the proposed scheme models are trained over 9 epochs as the forward iteration and 3 epochs for backwards iteration. We also expect that the proposed scheme models will also decrease with each epoch, meaning our model predicts value y more frequently and accurately as the model is further continued for training. The test graph also indicates that validation performance at epoch 3 prediction of the proposed models is a good one.



Algorithms

Data Division: Random (dividerand)
Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Calculations: MEX

9/100 Iterations

Progress

Epoch: 0 9 iterations 100
Time: 0:00:01
Performance: 14.8 0.00881 0.00
Gradient: 25.3 0.0320 1.00e-07
Mu: 0.00100 0.000100 1.00e+10
Validation Checks: 0 6 6

Validation Parameters

✓ Validation stop.

(**a**)

(**b**)

**Figure 8.** (**a**) Feed forward propagation structure; (**b**) Firefly back Propagation.

### 4.9. Identification of All Affected Nodes and Retrieval

The proposed research work scheme also presents a regression model with the back propagation, as shown in Figure 9.

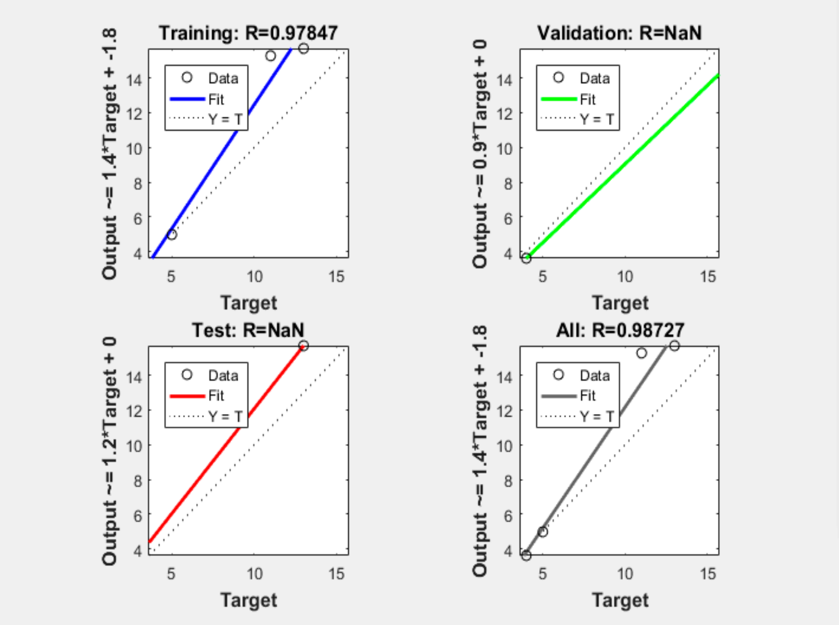


**Figure 9.** Regression model.

## 5. Analysis and Discussion of Results

From Figure 9, the regression model of the proposed scheme is evaluated. Based upon the evaluation, the training result is 0.7847, the validation result is NaN (not a number), the test result is NaN, and the overall result is 0.98727. These values represent close but high regression values. Generally, close but high regression values represents healthy training and classification structures. High regression values are also the reason that the prevention parameters of HDSA are high, including DoS JSA and other attack activities causing jitter and delay in the network.

As discussed earlier, this section classifies the path value on the basis of the trained structure. The identified malicious vehicle or node is always sent for recovery or maintenance. The following evaluations are also made.

### *5.1. Analysis of Jitter, Throughput, and Prediction Accuracy of the Proposed Scheme and the Other Contending Schemes*

Based upon the proposed scheme models and algorithms, comparison analysis is made with the other contending schemes, such as CUCKOO/Artificial Bee Colony (ABC) and Firefly/Genetic algorithm (GA) models and algorithms. We determined jitter, throughput, and the prediction accuracy. Based upon this, we evaluated end-to-end delay using attacked packet detection algorithms (APDA) and the models in the network, which detected HDSA, including DoS JSA and other attacks observed in the paths of vehicles traveling in the network. V2V, V2RSU, and RSU2V communication processes were utilized. We utilized the simulation with the APDA, including unicast and multicast/broadcast data transmission. We also utilized single next hop vehicle (SNHV) data transfer probability based upon the proposed scheme models (HDAM, and PSAM integrated with PESATRM) concerning the vehicle communication processes, which include V2V, V2RSU, and RSU2V communication. IEEE 802.11p beacon transmissions were utilized in the network, which is based upon DSRC technology.

Thus, the proposed scheme prevention performed in the network, compared with the prevention performed with the other contending schemes, including CUCKOO (ABC) and Firefly (GA), were evaluated based on Jitter, throughput, and prediction accuracy, as follows.

### *5.2. Jitter Analysis*

Figure 10 illustrates the Jitter for the proposed scheme versus two other schemes. Evaluating the Jitter, the proposed scheme jitter was compared to the other contending schemes, such as Firefly (GA) and CUCKOO (ABC). This evaluation was based upon the end-to-end delayed path of the vehicle communication process observed in the network. For the proposed scheme models, which include HDAM, PSAM, and the PESATRM communication process, the jitter is 60 ms less, whereas the jitter values for CUCKOO (ABC) and Firefly (GA) were 93 ms and 89 ms, respectively, which are high. This is because the proposed scheme architecture models utilized the training structure and did not have to compare the entire feature set, which consumes a lot of time in the case of HDSA, including DoS JSA and other threat detection, based upon the attacked packet transmitted in the model architecture. However, both Firefly (GA) and CUCKOO (ABC) are iterative in nature, and hence consume a lot of time. Mathematically, the jitter can be computed in Equation (19. The jitter comparison are given in Table 5. Table 6 shows the average jitter value for different schemes.

$$Avg_{Jitter} = \frac{Max_{Jitter} - Min_{Jitter}}{2} \tag{19}$$

**Table 5.** Jitter comparison.

| Iterations | Jitter-Proposed in ms | Jitter-Cuckoo in ms | Jitter-Firefly in ms |
|---|---|---|---|
| 100 | 12 | 23 | 26 |
| 500 | 16 | 35 | 42 |
| 1000 | 60 | 89 | 93 |

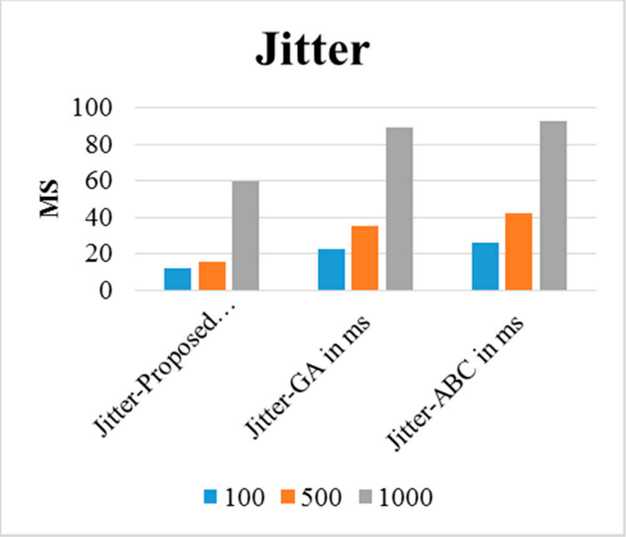


**Figure 10.** Jitter for the proposed scheme versus two other schemes.

**Table 6.** Average jitter value.

| | |
|---|---|
| Proposed Average Jitter | 24 |
| Firefly Average Jitter | 33 |
| CUCKOO Average Jitter | 33.5 |
| Proposed to FIREFLY | 72% |
| Proposed to CUCKOO | 71.64% |

$$\% \, Improvement = \frac{(Final \times 100)}{Initial} \tag{20}$$

### *5.3. Throughput Analysis*

The second evaluation is performed on the basis of throughput. As emphasized already, the throughput evaluation is also based upon the comparison of the proposed scheme with the other contending schemes, which are Artificial Bee Colony (CUCKOO) and Genetic Algorithm (Firefly) schemes. The throughput is determined using the formula as follows in Equation (21):

$$\text{Throughput} = \text{Tdp} \times \text{tm} \tag{21}$$

Tdp is the total delivered packets, and tm is total time tp transmit information from the transmitting vehicle or node to the receiving vehicle or node in the proposed scheme SAM. Table 7 shows the throughput.

**Table 7.** Throughput.

| Iteration Count | Throughput-Proposed | Throughput-CUCKOO | Throughput-Firefly |
|---|---|---|---|
| 100 | 523,300 | 235,411 | 365,412 |
| 500 | 652,311 | 352,210 | 356,221 |
| 1000 | 721,112 | 396,521 | 385,211 |

The proposed scheme algorithms and models, which include HDAM, PSAM, and PESATRM, utilize maximum time. This results in the least end-to-end delay of the path of the vehicles' jitter values. Thus, we envisage that time value is important and time value is utilized in transferring the data packets securely and efficiently. Hence, the proposed scheme models have resulted in a higher throughput value as compared to the other contending schemes, which are CUCKOO (ABC) and the Firefly (GA) scheme throughput, which are less.

### *5.4. Prediction Accuracy Analysis*

The third evaluation is also done on the basis of the prediction accuracy of the proposed scheme. It is also compared with the other contending schemes, including Artificial Bee Colony (CUCKOO) and Genetic Algorithm (Firefly) protocols. The prediction accuracy of the proposed scheme compared to the other contending schemes, which are CUCKOO (ABC) and the Firefly (GA), are determined as shown in Table 8.

**Table 8.** Prediction Accuracy.

| | |
|---|---|
| Proposed Scheme | 92% |
| Cuckoo | 63% |
| Firefly | 63.89% |

## 6. Miscellaneous

Table 9 provides a comparison of VANET protocols based on trustworthiness, attack detection, and mode of transmission.

**Table 9.** Summary of background study.

| Protocols | Data Transmission Mode | Performance Measurement for Accuracy and Trustworthiness | Attacks Detection | Storage and Authentication Mechanism |
|---|---|---|---|---|
| [9] RTMD | None | No trustworthiness and accuracy | Only DoS JSA | None |
| [10] FECM | None | No trustworthiness and prediction accuracy | Only DoS JSA | None |
| [11] DRIA | Unicast traffic mode | No trustworthiness and prediction accuracy | Only DoS JSA | None |
| [12] RTDD | Broadcast traffic mode | No trustworthiness and prediction accuracy | Only DoS JSA | None |
| [14] RTVA, and [17] EMDV | Mostly multicast | No trustworthiness and prediction accuracy | Only DoS JSA | VFC only and none |
| Proposed scheme protocol | Unicast, broadcast/multicast | Trustworthiness and prediction accuracy | HDSA, DoS JSA, PD, and RCRCO | VFC, HOA, and AKDE |

## 7. Conclusions

The vehicular ad hoc network (VANET) avoids heavy traffic conditions and driving problems that may be encountered on the roads, including highways. Due to the environment in which VANET is deployed, VANET encounters a lot of trustworthiness issues. This includes hybrid DoS attacks (HDSA), including DoS JSA and other forms of attacks that can be unpredictable with VANET. This leads to sporadic processing of information. Sporadic information processing prevents real-time information delivery in VANET during V2V, V2RSU, and RSU2V communication. Consequently, this introduces end-to-end delay and jitter in the network. Alleviating end-to-end delay and jitter in the network requires secure, efficient storage delivery and trustworthiness solutions.

This research has presented fog computing in a cloud-based integration (VFC) concept to secure VANET. The research also utilized hybrid optimization algorithms (HOAs), which are also intelligent and include CSA/ABC and Firefly/GA. HOAs are heuristics, and also have problem-solving skills. The HOAs integrate with vehicular authentication algorithms. In addition, they optimize FS and RSU further authentication algorithms, and also help to select trustworthy nodes in the network. This process has also led to secure transmissions of IEEE 802.11p beacon relays in VANET. Secure transmission helps to ensure safe V2V, V2RSU, and RSU2V VANET communication processes. VANET communication processes include standardized road safety information exchange (SRSIE). This requires VANET Infrastructure Architecture (VIA) system models.

In this research, the system architecture models of VIA and several interesting application scenarios, i.e., challenging issues of VFC, have been discussed in the proposed scheme. The proposed scheme VIA system models include HDAM, PSAM, and PESATRM. The HDAM is a hybrid model of two models that utilize the DoS attack model (DAM) and jamming signal attack model (DJSAM). These two attack models are used to identify and mitigate all forms of attacks, including HDSA, DoS JSA, and all other associated attacks. These HDSAs including DoS JSA and other attacks, interfere with IEEE 802.11p beacon transmission relays during V2V, V2RSU, and RSU2V information dissemination.

PSAM is the overall proposed scheme system model. PSAM utilizes attacked packet detection algorithms (APDA). APDA are used to identify the vehicle position and frequency of the number of attacked packets. PSAM utilizes multicast/broadcast and unicast modes of transmission of data, whilst utilizing the IEEE 802.11p beacons and signals for real-time data delivery. The PSAM also integrates with the PESATRM to provide robustness in VIA deployment. This integration model serves as an additional model of the proposed scheme and utilizes efficient ESATR to process V2V, V2RSU, and RSU2V communication of SRSIE. The PSAM and PESATRM integration models also provides further secure authentication and key distribution establishment (AKDE) for the RSU and the FS. This secures the network for trustworthiness. In addition, PESATRM utilizes probability analysis and also encompass NSHV and non-shadow environment encryption (NESE) concepts of VFC communication. This provide secure and SRSIE to sensitize the vehicles that move in the same transmission range in order to effectively prevent road casualties in a timely manner.

VFC integration with HOA and AKDE support rising VANET applications that demand predictable results with minimum energy consumption rate. This paper has focused on the dual training mechanism of Firefly (GA)/FFBP-NN to provide prevention and recovery mechanisms for all malicious node detection paths for end-to-end delay paths observed in VANET. It also reduced jitter in the proposed scheme significantly. As a result, the detection and prevention of all forms of attacks, such as HDSAs, including DoS JSA and other attacks, is high. Based upon this, the proposed scheme prediction accuracy is 92%. The proposed scheme uses the concepts of authentication and encryption and trustworthiness of nodes. The network provision also utilize hybrid information broadcast/multicast and unicast in the VANET. However, compared to Cuckoo (ABC) and Firefly (GA), their prediction accuracies are, respectively, 63% and 63.89%. These schemes have limitations in trustworthiness provision in VANET. They do not utilize HOAs and AKDE.

In addition, the proposed scheme algorithm and the models, which include HDAM, PSAM, and PESATRM, significantly contributed to efficiently reducing the jitter value by 72%. The maximum attained throughput for the proposed scheme is importantly high as compared to Cuckoo (ABC) and Firefly (GA). The paper utilized FFBP-NN over 100 iterations, out of which 30–40 iterations are reserved for Firefly back propation.

In our future work, we would like to design the layout and implementation of VANET, which would also involve other forms of optimization techniques, including the Spline method to minimize the jitter problems in the fog computing environment. Then, performance evaluation based upon different forms of attacks in the network, including HDSA, would also be assessed.

**Author Contributions:** Conceptualization, S.E. and K.E.; Methodology, S.E. and K.E.; Validation, S.E.; Writing—original draft, S.E.; Writing—review & editing, K.E.

**Funding:** This research has been sponsored by the University of Bridgeport.

**Acknowledgments:** The authors Samuel Kofi Erskine and Khaled M. Elleithy acknowledge that the formulae and algorithms developed in this research were solely their own work.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References

1. Singh, D.; Ranvijay; Yadav, R.S. A state-of-art approach to misbehavior detection and revocation in VANET: Survey. *Int. J. Ad Hoc Ubiquitous Comput.* **2018**, *28*, 77–93. [CrossRef]
2. Cooper, C.; Franklin, D.; Ros, M.; Safaei, F.; Abolhasan, M. A Comparative Survey of VANET Clustering Techniques. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 657–681. [CrossRef]
3. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANet security challenges and solutions: A survey. *Veh. Commun.* **2017**, *7*, 7–20. [CrossRef]
4. Sharma, S.; Kaul, A. A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud. *Veh. Commun.* **2018**, *12*, 138–164. [CrossRef]
5. Campolo, C.; Molinaro, A. Multichannel communications in vehicular Ad Hoc networks: A survey. *IEEE Commun. Mag.* **2013**, *51*, 158–169. [CrossRef]
6. Campolo, C.; Molinaro, A.; Vinel, A.; Zhang, Y. Modeling Prioritized Broadcasting in Multichannel Vehicular Networks. *IEEE Trans. Veh. Technol.* **2012**, *61*, 687–701. [CrossRef]
7. Anbuchelian, S.; Lokesh, S.; Baskaran, M. Improving Security in Wireless Sensor Network Using Trust and Metaheuristic Algorithms. In Proceedings of the 2016 3rd International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, Malaysia, 5–17 August 2016; pp. 233–238.
8. Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S.V. Denial of Service Attacks in Wireless Networks: The Case of Jammers. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 245–257. [CrossRef]
9. Tang, J.; Cheng, Y.; Zhuang, W. Real-time misbehavior detection in IEEE 802.11 based wireless networks: An analytical approach. *IEEE Trans. Mob. Comput.* **2014**, *13*, 146–158. [CrossRef]
10. Djahel, S.; Zhang, Z.; Nait-Abdesselam, F.; Murphy, J. Fast andefficient countermeasure for MAC Layer misbehavior in MANETs. *IEEE Wirel. Commun. Lett.* **2012**, *1*, 540–543.

11. Hamieh, A.; Ben-othman, J.; Mokdad, L. Detection of radio interference attacks in VANET. In Proceedings of the 2009 IEEE Global Telecommunications Conference, Honolulu, HI, USA, 30 November–4 December 2009. [CrossRef]
12. Lyamin, N.; Vinel, A.; Jonsson, M.; Loo, J. Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks. *IEEE Commun. Lett.* **2014**, *18*, 110–113. [CrossRef]
13. Kolesnikov, V.; Lee, W.; Hong, J. MAC aggregation resilient to DoS attacks. In Proceedings of the Cyver Physical Security and Privacy (IEEE 2011 smart GridComm), Brussels, Belgium, 17–20 October 2011; pp. 226–228.
14. Grover, J.; Jain, A.; Singhal, S.; Yadav, A. Real-Time VANET Applications Using Fog Computing. In *Proceedings of First International Conference on Smart System, Innovations and Computing. Smart Innovation, Systems and Technologies*; Springer: Singapore, 2018; pp. 683–685.
15. Narawade, V.E.; Kolekar, U. EACSRO: Epsilon constraint-based Adaptive Cuckoo Search algorithm for Rate Optimized Congestion Avoidance and Control in Wireless Sensor Networks. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 715–720.
16. Kaur, G. A preventive approach to mitigate the effect of gray hole using genetic algorithm. In Proceedings of the 2016 IEEE International Conference on Advanced in Computing, Communication, Automation (ICACCA), Dehradun, India, 8–9 April 2016; pp. 1–2.
17. Ghaleb, F.A.; Zainal, A.; Rassam, M.A.; Mohammed, F. An effective misbehavior detection model using artificial neural network for vehicularad hoc network applications. In Proceedings of the 2017 IEEE Conference on Application, Information and Network Security (AINS), Miri, Malaysia, 13–14 November 2017.
18. Zhang, R.; Jiang, X.; Li, R. Decomposition based multiobjective spectrum allocation algorithm for cognitive vehicular networks. In Proceedings of the 2017 IEEE 17th International Conference on Communication Technology (ICCT), Chengdu, China, 27–30 October 2017; pp. 831–836.
19. Saoucha, N.A.; Ghanem, K.; Benmammar, B. On applying Firefly Algorithm for Cognitive Radio Networks. In Proceedings of the 2014 IEEE 21st Symposium on Communications and Vehicular Technology in the Benelux (SCVT), Delft, The Netherlands, 10 November 2014; pp. 1–2.
20. Kushwah, N.; Sonker, A. Malicious Node Detection on Vehicular Ad-Hoc Network Using Dempster Shafer Theory for Denial Of Services Attack. In Proceedings of the 2016 IEEE International Conference on Computational Intelligence and Communication Networks, Tehri, India, 23–25 December 2016; pp. 432–433.
21. Waraich, P.S.; Batra, N. Prevention of Denial of Service Attack Over Vehicle Ad hoc Networks using Quick Response Table. In Proceedings of the 2017 IEEE International Conference on Signal processing, Computing and Control (ASPCC), Solan, India, 21–23 September 2017; pp. 586–587.
22. Sedjelmaci, H.; Senouci, S.M.; Abu-Rghef, M.A. An Efficient and Lightweight Intrusion Detection Mechanism for Service-Oriented Vehicular Networks. *IEEE Internet Things J.* **2014**, *1*, 570–577. [CrossRef]
23. Shabbir, M.; Khan, M.A.; Khan, U.S.; Saqib, N.A. Detection and Prevention of Distributed Denial of Service Attacks in VANETs. In Proceedings of the IEEE 2016 International Conference on Computational Science and Computational Intelligence, Las Vegas, NV, USA, 15–17 December 2016; pp. 970–971.
24. Sharma, S.; Kaul, A. Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized IDS for VANET. *Veh. Commun.* **2018**, *12*, 23–38. [CrossRef]
25. Jiang, Q.; Ni, J.; Ma, J.; Yang, L.; Shen, X. Integrated Authentication and Key Agreement Framework for Vehicular Cloud Computing. *IEEE Netw.* **2018**, *32*, 28–35. [CrossRef]
26. Agarwal, Y.; Jain, K.; Karabasoglu, O. Smart vehicle monitoring and assistance using cloud computing in vehicular Ad Hoc networks. *Int. J. Transp. Sci. Technol.* **2018**, *7*, 60–73. [CrossRef]
27. Glass, S.; Mahgoub, I.; Rathod, M. Leveraging MANET-Based Cooperative Cache Discovery Techniques in VANETs: A Survey and Analysis. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2640–2661. [CrossRef]
28. Chaba, S.; Kumar, R.; Pant, R.; Dave, M. Secure and efficient key delivery in VANET using cloud and fog computing. In Proceedings of the 2017 International Conference on Computer, Communications and Electronics (Comptelix), Jaipur, India, 1–2 July 2017; pp. 27–31.

29. Sookhak, M.; Yu, F.R.; Tang, H. Secure data sharing for vehicular ad-hoc networks using cloud computing. In *Ad Hoc Networks*; Springer: Cham, Switzerland, 2016; pp. 306–315.
30. Kumar, R.; Chhabra, S. Efficient routing in Vehicular Ad-hoc Networks using Firefly optimization. In Proceedings of the 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 26–27 August 2016; pp. 1–6.
31. Fekair, M.E.A.; Lakas, A.; Korichi, A. CBQoS-Vanet: Cluster-based Artificial Bee Colony Algorithm for QoS Routing Protocol in VANET. In Proceedings of the 2016 International Conference on Selected Topics in Mobile & Wireless Network (MoWNeT), Cairo, Egypt, 11–13 April 2016; pp. 1–3.
32. Khalil, M.; Azer, M.A. Sybil attack Prevention through Identity Symmetric Scheme in Vehicular Ad hoc Networks. In Proceedings of the IEEE 2018 Wireless days (WD), Dubai, UAE, 3–5 April 2018; pp. 184–185.
33. Roselin Mary, S.; Maheshwari, M.; Thamaraiselvan, M. Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA). In Proceedings of the 2013 IEEE International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 21–22 February 2013; pp. 237–240.
34. Verma, K.; Hasbullah, H. IP-CHOCK (filter)-Based Detection Scheme for Denial of Service (DoS) attacks in VANET. In Proceedings of the 2014 International Conference Computer and Information Sciences (ICCOINS), Kuala Lumpur, Malaysia, 3–5 June 2014; pp. 1–6.
35. Quyoom, A.; Ali, R.; Gouttam, D.N.; Sharma, H. A Novel Mechanism of Detection of Denial of Service Attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA). In Proceedings of the International Conference on Computing, Communication and Automation (ICCCA2015), Noida, India, 15–16 May 2015; pp. 414–416.
36. Ekici, E.; Heijenk, G.; Jarupan, B.; Weil, T.; Karagiannis, G.; Altintas, O.; Lin, K. Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 584–616.
37. Lai, Y.; Zhang, L.; Wang, T.; Yang, F.; Xu, Y. Data Gathering Framework Based on Fog Computing Paradigm in VANETs. In *Asia-Pacific Web (APWeb) and Web-Age Information Management (WAIM) Joint Conference on Web and Big Data*; Springer: Cham, Switzerland, 2017; pp. 227–236.
38. Khan, A.A.; Abolhasan, M.; Ni, W. 5G next generation VANETs using SDN and fog computing framework. In Proceedings of the 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 12–15 January 2018; pp. 1–6.
39. Kaiwartya, O.; Kumar, S.; Lobiyal, D.K.; Abdullah, A.H.; Hassan, A.N. Performance Improvement in Geographic Routing for Vehicular Ad Hoc Networks. *Sensors* **2014**, *14*, 22342–22371. [CrossRef] [PubMed]
40. Buttner, C.; Bartels, F.; Huss, S.A. Real-World Evaluation of an Anonymous Authenticated Key Agreement Protocol for Vehicular Ad-Hoc Networks. In Proceedings of the 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, UAE, 19–21 October 2015; pp. 652–654.
41. Raw, R.S.; Das, S. Performance analysis of P-GEDIR protocol for vehicular *adhoc* network in urban traffic environments. *Wirel. Pers. Commun.* **2013**, *68*, 65–78. [CrossRef]
42. Yang, J.; Fei, Z. Broadcasting with Prediction and Selective Forwarding in Vehicular Networks. *Int. J. Distrib. Sens. Netw.* **2013**, *1*, 1–9. [CrossRef]
43. Artimy, M. Local Density Estimation and Dynamic Transmission-Range Assignment in Vehicular *Ad Hoc* Networks. *IEEE Trans. Intell. Transp. Syst.* **2007**, *8*, 400–412. [CrossRef]
44. Erskine, S.K.; Elleithy, K.M. Secure Intelligent Vehicular Network Using Fog Computing. *Electronics* **2019**, *8*, 455. [CrossRef]
45. Cuevas, E.; Reyna-Orta, A. A Cuckoo Search Algorithm for Multimodal Optimization. *Sci. World J.* **2014**, *2014*, 20. [CrossRef]
46. Vinel, A.; Campolo, C.; Petit, J.; Koucheryavy, Y. Trustworthy Broadcasting in IEEE 802.11p/WAVE Vehicular Networks: Delay Analysis. *IEEE Commun. Lett.* **2011**, *15*, 1010–1012. [CrossRef]
47. Wu, Q.; Liu, Q. A Trusted Routing Protocol Based on Bayesian in VANET. In Proceedings of the IEEE 2014 International Conference on Cyberspace technology (CCT), Beijing, China, 8–10 November 2014; pp. 1–4.

48. Huang, N.J.; Wang, X. Vehicular Fog Computing: Enabling Real-Time Traffic Management for Smart Cities. *IEEE Wirel. Commun.* **2019**, *26*, 87–93.
49. Hasan, K.F.; Wang, C.; Feng, Y.; Tian, Y.C. Time synchronization in vehicular ad-hoc networks: A survey on theory and practice. *Veh. Commun.* **2018**, *14*, 39–51. [CrossRef]