

SECURE INTELLIGENT VEHICULAR NETWORK  
INCLUDING REAL-TIME DETECTION OF DoS ATTACKS IN  
IEEE 802.11P USING FOG COMPUTING

Samuel Kofi Erskine

Under the Supervision of: Dr. Khaled Elleithy

DISSERTATION  
SUBMITTED IN PARTIAL FULFILMENT FOR REQUIREMENTS  
FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE  
AND ENGINEERING  
THE SCHOOL OF ENGINEERING  
UNIVERSITY OF BRIDGEPORT  
CONNECTICUT  
May 2020



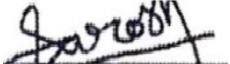
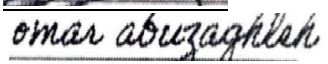

**SECURE INTELLIGENT VEHICULAR NETWORK**  
**INCLUDING REAL-TIME DETECTION OF DoS ATTACKS IN**  
**IEEE 802.11P USING FOG COMPUTING**

Samuel Kofi Erskine

Under the Supervision of Dr. Khaled Elleithy

**Approvals**

**Committee Members**

<b>Name</b>	<b>Signature</b>	<b>Date</b>
Dr. Khaled Elleithy		<u>8/24/2020</u>
Dr. Prabir Patra		<u>8/24/2020</u>
Dr. Sarosh Patel		<u>8/24/2020</u>
Dr. Omar Abuzaghleh		<u>8/24/2020</u>
Dr. Syed Rizvi		<u>8/24/2020</u>

**Ph.D. Program Coordinator**

Dr. Khaled M. Elleithy		<u>8/24/2020</u>
------------------------	--	------------------

**Chairman, Computer Science and Engineering Department**

Dr. Ausif Mahmood		<u>8/23/2020</u>
-------------------	--	------------------

**Dean, School of Engineering**

Dr. Khaled M. Elleithy		<u>8/24/2020</u>
------------------------	--	------------------

SECURE INTELLIGENT VEHICULAR NETWORK  
INCLUDING REAL-TIME DETECTION OF DoS ATTACKS IN  
IEEE 802.11P USING FOG COMPUTING

**ABSTRACT**

VANET (Vehicular ad hoc network) has a main objective to improve driver safety and traffic efficiency. Intermittent exchange of real-time safety message delivery in VANET has become an urgent concern, due to DoS (Denial of service), and smart and normal intrusions (SNI) attacks. Intermittent communication of VANET generates huge amount of data which requires typical storage and intelligence infrastructure. Fog computing (FC) plays an important role in storage, computation, and communication need.

In this research, Fog computing (FC) integrates with hybrid optimization algorithms (OAs) including: Cuckoo search algorithm (CSA), Firefly algorithm (FA) and Firefly neural network, in addition to key distribution establishment (KDE), for authenticating both the network level and the node level against all attacks for trustworthiness in VANET. The proposed scheme which is also termed “Secure Intelligent

Vehicular Network using fog computing” (SIVNFC) utilizes feedforward back propagation neural network (FFBP-NN). This is also termed the firefly neural, is used as a classifier to distinguish between the attacking vehicles and genuine vehicles. The proposed scheme is initially compared with the Cuckoo and FA, and the Firefly neural network to evaluate the QoS parameters such as jitter and throughput.

In addition, VANET is a means whereby Intelligent Transportation System (ITS) has become important for the benefit of daily lives. Therefore, real-time detection of all form attacks including hybrid DoS attacks in IEEE 802.11p, has become an urgent attention 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 enormous amount of message. This leads to the RSU (roadside unit) or the CPU (central processing unit) overutilization for computation. Therefore, it is required that efficient storage and intelligence VANET infrastructure architecture (VIA), which include trustworthiness is desired. Vehicular Cloud and Fog Computing (VFC) play an important role in efficient storage, computations, and communication need for VANET.

This dissertation also utilizes VFC integration with hybrid optimization algorithms (OAs), which also possess swarm intelligence including: Cuckoo/CSA Artificial Bee Colony (ABC) Firefly/Genetic Algorithm (GA), in additionally to provide Real-time Detection of DoS attacks in IEEE 802.11p, using VFC for Intelligent Vehicular network. Vehicles are moving with certain speed and the data is transmitted at 30Mbps. Firefly FFBPNN (Feed forward back propagation neural network) has been used as a classifier to also distinguish between the attacked vehicles and the genuine vehicle. The proposed

scheme has also been compared with Cuckoo/CSA ABC and Firefly GA by considering Jitter, Throughput and Prediction accuracy.

## **DEDICATION**

*This dissertation is dedicated to loved ones: Jude and Junior (my sons), Godlove and Sonary (my daughters). It is also dedicated to Hannah as loved one. Other dedication is due on my parents, my father Christian (who has passed away soul) and Mother Christina and my siblings, without the help and support of your prayers and of kind of these loved ones, it would be difficult to attain this level in my education.*

## **ACKNOWLEDGEMENTS**

To Almighty God I wholly devote thanksgiving. To God Alone Be the Glory, honor, and adoration. For it is in Him alone I derived source of inspiration, and who has helped me to be successful in this dissertation work.

I am also indebted to Dr. Khaled Elleithy, who is my professor and advisor who supervised my work. His continued support, advice and a lot of forbearance exhibited, right from the very beginning of this PhD dissertation, till this time of submitting this dissertation. This great achievement would be difficult without his selfless support. I express my profound gratitude toward his remarkable expertise shown towards providing me such a high quality of work. This positively reflected on the praise received from expert and committee for this dissertation who once reviewed this work.

My gratitude also goes to all the committee members on their positive comments, advice and constructive evaluations and encouragements to me: Dr Prabir Patra, Dr. Syros Patel and Dr. Omar Abuzegleh. I also express my profound appreciation to Dr. Syed Rizvi who is the external member of the dissertation advisory committee, for his invaluable commitment, time and evaluation spent on my work.

To be able to come this far and to the end of this journey was no small achievement. However, one thing realized is that it is not your hard work or your smartness that makes

you successful. You cannot simply achieve success without the inclusion of great supporters. The support from home based on other loved relatives and the support received from school was invaluable. I express my gratitude to other professors of the department of Computer Science and Engineering at University of Bridgeport for their enormous support and encouragement given to me. It was a great pleasure either working for them or participated in their class.



## ACRONYMS

$d_p$	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

---

# TABLE OF CONTENTS

Abstract.....	iii
DEDICATION .....	v
ACKNOWLEDGEMENT.....	vi
ACRONYM .....	viii
TABLE OF CONTENT.....	x
LIST OF TABLES.....	xiii
LIST OF FIGURES.....	xiv
<b>CHAPTER 1: INTRODUCTION .....</b>	<b>1</b>
1.1 Research Problem and Scope .....	1
1.2 Motivation Behind The Research .....	4
1.3 Potential Contribution of The Research .....	7
<b>CHAPTER 2: SECURING VANETS ARCHITECTURES.....</b>	<b>8</b>
2.1. Securing VANETs-Fog Centric Distributed Architecture .....	10
2.2. Securing VANETs-Centralized Architect based on DoS Attacks and related attack.....	13
2.3. Securing the VANETs-Fog Computing (VFC) Using Cloud Centric Architecture.....	17
<b>CHAPTER 3: DOS ATTACKS AND PREVENTIVE MECHANISM IN VANET.....</b>	<b>23</b>
3.1. DoS Attack.....	23
3.2 Attack Principle.....	24
3.3. DoS Attack Illustration.....	26
3.4. Intrusion/Attack Model .....	27

3.4.1. Smart & Normal Intrusion Attack Scenario.....	29
<b>CHAPTER 4: MATHEMATICAL AND IMPLEMENTATION .....</b>	<b>31</b>
4.1. Proposed System Architecture Prevention Model (SAPM).....	31
4.2. DDoS SAPM.....	35
4.3. Fog Server (FS-L) Preventive Mechanism.....	37
4.4. Fog Computing Storage Preventive Model.....	41
4.5. Communication Cost Model.....	43
4.6. Node Level Security.....	47
4.7. RSU-L Prevention Mechanism.....	48
4.8. Identification of Affected Node and Recovery.....	54
<b>CHAPTER 5: RESULT ANALYSIS AND DISCUSSION.....</b>	<b>55</b>
5.1. Feed forward Backwards Propagation Regression Model Result and Analysis.....	55
5.1.1. Feed forward backward Propagation.....	55
5.1.2. Regression Model Result and Analysis.....	56
5.2. QoS Provision Analysis in VANET.....	56
5.2.1. QoS Result and Analysis of the Proposed Scheme.....	57
<b>CHAPTER 6: REAL TIME DETECTION OF DOS ATTACKS IN IEEE 802.11P USING FOG COMPUTING FOR SECURE INTELLIGENT VEHICULAR NETWORK.....</b>	<b>62</b>
6.1 Introduction.....	62
6.1.1 Background Study of the Research.....	65
6.2 Secure Real time Detection of DoS Attacks Preventive Measures in VANET.....	70
6.2.1: Hybrid DoS Attacks (HDSA).....	70
6.3. DoS Attacks and Models .....	71
6.3.1 Packet Drop (PD) and False Information (FI).....	74
6.3.2. DoS Jamming Signal Attacks (DoSJSA) .....	75
6.4 Prevention Mechanism of the proposed Scheme .....	77

6.4.1 Proposed Scheme System Architecture Model .....	77
6.5 Fog Computing Storage Preventive Model .....	85
6.6 Elliptical Segment Area Transmission Range and Authentication Preventive Model.....	88
6.6.1 Fog Server Further Authentication Process in Elliptical Area .....	94
6.6.2 Probability Analysis of Vehicle on Elliptical Segment Area Transmission range.....	97
6.7. Trust Provision Model in VANET.....	103
6.8. RSU Network Prevention Mechanism against Hybrid DoS Attack .....	105
6.8.1. Modelling of DoS Threat Prevention.....	107
6.8.2 Identification of all Affected and Retrieval Nodes.....	114
6.9. Results Analysis and Discussion.....	115
6.9.1 Analysis of Jitter Throughput and Prediction Accuracy of the Proposed Scheme and Other Models.....	116
6.9.2 Jitter Analysis .....	116
6.9.3 Throughput Analysis .....	119
6.9.4 Prediction Accuracy Analysis .....	119
<b>CHAPTER 7: CONCLUSION AND FUTURE WORK.....</b>	<b>122</b>

## LIST OF TABLES

Table 4	Specification Considered for Cuckoo Search Algorithm.....	40
Table 4.7	Network Specification.....	48
Table 4.7.1	Utilized Feedforward Back Propagation Structure.....	51
Table 5.2	Throughput of Proposed Scheme Compared to Others at Various PIR.....	59
Table 5.2.1	Jitter of Proposed Scheme Compared to Others at Various PIR.....	61
Table 6.6	Cuckoo Specification.....	101
Table 6.8.1	Firefly Uses FFBP-NN Structure.....	109
Table 6.8.2	Further Acronyms.....	111
Table 6.9.2	Jitter Comparison .....	117
Table 6.9.4	Percentage Jitter Improvement of Proposed Scheme to other Schemes.....	118
Table 6.9.5	Throughput.....	119
Table 6.9.6	Prediction Accuracy.....	120
Table 6.9.7	Summary of Background Study of VANET Protocols Based on Trustworthiness, Attack Detection and Mode of Transmission .....	120

## LIST OF FIGURES

Figure 3.2	Channel occupancy.....	24
Figure 3.2.1	Intrusion Attacker Model .....	27
Figure 3.4.1	Normal/Smart Intrusion .....	29
Figure 4.1.	Proposed System Architecture Model (SIVNFC).....	32
Figure 4.1.1	VANET Structure with Integrated Fog Server.....	34
Figure 4.2	DDoS Attack Including SNI Attack DoS Mitigation.....	35
Figure 4.3	Node Communication with Fog Server .....	41
Figure 4.5	Degree of Membership Versus QoS Awareness .....	46
Figure 4.7a	Constructed Vehicle Path.....	50
Figure 4.7b	Attacker /Intrusion Path.....	51
Figure 4.7.1a	Feed Forward Structure.....	52
Figure 4.7.1b	Back Propagation Firefly.....	52
Figure 4.8	Regression Model.....	54
Figure 5.2	Throughput Versus PIR.....	58
Figure 5.2.1	Jitter Versus PIR.....	60
Figure 6.0	VANET Infrastructure Architecture.....	63
Figure 6.3	Hybrid DoS Attack Model (DAM).....	72
Figure 6.3.2	Vehicular Communication Jamming Signal Attack Model.....	76
Figure 6.4.1	Proposed System Architecture Model.....	79

Figure 6.4.2	Authentication of Data Packet Using Vehicular RSA.....	84
Figure 6.6	Vehicles in Elliptical Segment Transmission range Model.....	93
Figure 6.8.1a	Path Construction of Vehicles .....	107
Figure 6.8.1b	Malicious nodes/Intrusion attack path.....	108
Figure 6.8.1.2a	Feed Forward Propagation Structure.....	113
Figure 6.8.1.2b	Back Propagation Fire Flyton.....	113
Figure 6.8.2	Regression Model.....	114
Figure 6.9.2	Jitter For The Proposed Scheme Versus two Other Scheme.....	118



# CHAPTER 1: INTRODUCTION

## 1.1 Research Problem and Scope

It is noticeable that the automation industry has substantially improved in the last couple of years. The integration of hardware and software components produces better drivability and customer satisfaction. A vehicular ad hoc network (VANET) contains mobile vehicles with on-board processing units (OBPU) and roadside units (RSUs) that assist vehicles [1–3]. Vehicle-to-vehicle (V2V) communication is fortified to provide improved information to the drivers regarding roadside accidents, traffic jams, etc. This improves driver safety and the driving comfort of the vehicle in city traffic and on highways [4]. Highways, crossroads conditions, weather conditions, and vehicles monitoring are now part of the VANET important safety applications that must be complied. Examples of the safety applications include: Slow stop vehicle advisor (SSVA), post-crash notifications (PCN), and collision/congestion avoidance (CCA).

These safety applications are important for VANET. VANET utilizes these safety applications to acquire prior knowledge of crossroads, highways, and knowledge of other vehicles conditions. In addition, safety applications enable drivers to execute sound judgment. Through safety applications, drivers are capable to obtain real-time information needed in order to enable them to initiate logical judgment and prevent further road and

highway accidents occurrence. Regarding SSVA, vehicles that have slowed down or halted convey messages or information while utilizing warning signals message received from the network and take appropriate action.

The warning signal messages sensitizes the surrounding Vehicles in VANET that may be in danger. With regard to PCN, messages are conveyed to highway patrols for further assistance through neighboring vehicles. Neighboring vehicles are closer to each other such that trust establishment in them becomes an urgent issue with VANET. The trust gained through neighboring nodes would enable them to acquire accurate and real-time information of accidents and any emergency situation on roads.

It will also identify any denial of service (DoS) and intrusions on emergency activities that may have been encountered in the network. Moreover, safety applications such as SSVA, PCN, and CCA are connected with the RSU and are also deployed in VANET and connected at the traffic management office (TMO). However, the connection of these safety applications with the RSU requires improvement and efficient information delivery. The safety applications and the network devices can function appropriately and also ensure timely notifications about any accidents and road emergency situations. In addition, installation of VANET and appropriate deployment of the RSU with safety applications can help disseminate and process warning messages accurately in real-time without delay.

Moreover, it is anticipated that warning messages can be conveyed in a timely manner through the VANET, through which the message can be relayed to other vehicles. The warning messages are usually generated at the TMO and may include notifications of

DoS and intrusion attack activity in the network. Some of the DoS and intrusion attacks include congestion/collision (CC), link breakdown, and bad road conditions. CC of vehicles can occur in VANET at any time on the road due to the behavior of the disabled vehicle or accident which requires immediate attention and notification on a timely basis.

In addition, some DoS intrusion attacks which this research investigates include smart and normal intrusions (SNI) attacks. DoS and SNI attacks may cause link breakdowns in the network. DoS and SNI attacks also overwhelm the network and block the entire V2V communication within VANET. DoS and SNI attacks encountered in VANET become road threats. When these occur, they prohibit VANET safety applications to function appropriately. In addition, they may lead to further attacks in VANET, including the bad road conditions and highway congestion encountering of many vehicles.

This will also make it difficult for drivers to prevent road casualties in a timely manner. DoS, SNI, and DRA (DoS resilience attacker) all have the tendency to overwhelm the RSU. DoS and SNI can also exploit the RSU computational and communication resources and cause flooding with any requested information. However, the intent of RSUs and their deployed safety applications is to be able to collect and analyze the real-time information from vehicles. The information that is eventually received by V2V communication should be appropriately analyzed and evenly distributed to other neighboring vehicles, connected through VANET and safety applications on timely manner through the end-to-end (E2E) communication process.

The E2E communications process in VANET is important; however, E2E communication may experience particular DoS and SNI attacks which can also overwhelm

the RSU, which would then require urgent attention. The RSU may waste computational time, especially when it encounters false message or information. Therefore, the RSU requires an efficient and secure storage method to safeguard it from being compromised when delivering vehicle to roadside unit (V2RSU) and V2V messages in VANET [5].

## **1.2 Motivation behind the Research**

In VANET, V2V and V2RSU communication storage solutions for propagating safety information to nearby vehicles in a timely manner have been investigated using vehicular cloud and fog computing (VCF) [6]. The VCF model has been developed to utilize VANET resources efficiently due to fog computing (FC) and cloud-based logical interaction. Based upon VCF, grouped vehicles cooperate and communicate with each other and dynamically share sensing, computation, and resources for decision-making on the road, as well as for improving traffic management and road safety. There are some examples of VCF applications that can be relied upon which include:

- Collecting local and highways traffic conditions from neighboring vehicles for planning routes.
- Processing the big data traffic information through local and highway traffic management authorities.
- Critical collaborative events including road congestion, accidents, and all forms of attacks (including DoS and SNI attacks) can be reconstructed.

Although these applications scenarios have utilized FC and cloud-based applications for efficient storage and computations, this scheme has not been appropriately

secured. The authors claim that their proposed scheme has achieved their aim in investigating quality of service (QoS) parameters in VANET. Arguably, due to undetected DoS and SNI attacks, further investigation is needed. We believe fog computing (FC) integration and the hybrid deployment of optimization algorithms (OAs) including Cuckoo search algorithms (CSA), firefly algorithms (FA), firefly neural networks, and key distribution establishment (KDE)/authentication sharing mechanisms is a promising solution for investigating real-time data transmission and QoS parameters in VANET that answers to this question very well.

Thus, we believe integration of the KDE/authentication mechanism investigation for the network level and the node level security can be achieved appropriately in order to ensure trustworthiness of nodes and trustworthiness for the entire VANET. In addition, since RSUs play a major role in distributing information in VANET, they can be secured appropriately to provide real-time end-to-end V2V and V2RSU communication. Therefore, it has become urgent to investigate QoS parameters such as delay/jitter and throughput in VANET. Moreover, due to the dynamic nature of VANET, it utilizes a vulnerable wireless link. Wireless link deployment and connection with vehicles and associates connect through multimedia safety applications should be secured when vehicles connect with the RSU [7].

Since multimedia safety applications are now a part of the VANET system, however, they are easily plagued by DoS and SNI attacks through the RSU. Multimedia safety framework demands high QoS support and evaluation. QoS provision, in general, is required to supports the Media Access Control (MAC) architectures [8]. MAC architectures

for VANET rely on the VANET wireless medium which can be implemented on DSRC (dedicated short range communication) data link technology [9]. In the past, researchers/authors have conducted several investigations on VANET. The authors' investigation centered on multimedia safety application framework for determining QoS provision in VANET, which also utilized FC for achieving the network level security protection, using the DSRC data link technology.

In addition, the authors have conducted separate investigations on OAs based upon FC while utilizing DSRC data link technology for data transmission. The authors' investigation involved CSA [10–12], FAs [13–15] and a firefly neural network [16]. The aim of the authors was to evaluate QoS parameters for delay/jitter and throughput in VANET. In addition, during the research investigation, a firefly neural network was used to train effective misbehavior of the path delayed in the VANET. Though the authors claimed to have succeeded investigating QoS performance in the network, the QoS evaluation was not complete due to the inability of the researchers/authors to consider the node level security evaluation in VANET.

Moreover, the authors did not investigate KDE sharing, including hybrid integration with OAs. Therefore, there was a limitation in the evaluation of trustworthiness in VANET, and both real-time information delivery and QoS provision within VANET remain a major concern. FC integration with OAs including KDE sharing can be useful for implementing VANET safety applications, since these schemes have the capability to ensure efficient storage, time sensitivity, trustworthiness, and intelligence in real-time information delivery agendas and QoS in Intelligent Transportation systems. To

address these concerns, in this dissertation, we propose a “Secure Intelligent Vehicular Network using fog computing” (SIVNFC) scheme for FC integration and hybrid OAs deployment including CSA, FA, firefly neural networks, and KDE/authentication to detect the network level and node level security in VANET against DoS, SNI, and other forms of attacks.

### **1.3 Potential Contribution of the Research**

- Fog computing (FC) is integrated with hybrid OAs deployment including CSA, FA, firefly neural networks, and KDE. FC is used to determine the rapidly stored vehicular information. In addition, the integration and deployment of FC with hybrid OAs and KDE provides intelligence which reduces the search space for real-time information. It also prevents increased communication times. Fog computing is an extension of cloud computing that provides computation, storage services, and network communication services between the end nodes. The determination of the rapidly stored vehicular information process relies on the communication behavior of vehicles in [17].

- Secure the VANET at the node level and the network level for trustworthiness.
- Determine reduced jitter and improved throughput for the VANET for real-time data transmission.
- Use of regression model to confirm the accuracy of jitter/delay in the proposed SIVNFC scheme as a road safety application.

## CHAPTER 2: SECURING VANETS ARCHITECTURES

The architecture of VANETs and their operations are comprehensively analyzed in the literature [18]. The data sharing and key distribution mechanism during the data transfer were studied in [19]. Route discovery mechanisms were also developed and presented in the same scenario. We classify the security scenario at two levels: The security at the node level and the security at the network level. The node level security is applied when the selection of the node for the data transfer is involved, such as trusted node selection and the application of location-aware services [20].

In [21], the authors proposed location information verification cum security using a transferable belief model (TBM) for Geocast routing in VANET at the network level security. The proposed protocol included two level of location information verification. In the first level, tile-based techniques were used to verify location information correctness, whilst in level 2, collective information concerning the announced location information for each vehicle was obtained using TBM with the help of neighbor list information through all neighbor vehicles. The limitation of the proposed protocol is that it did not recommend any method for the network level security in order to evaluate trustworthiness in VANET. Rather, the proposed protocol only disputed traditional security methods and only proposed location information verification that was transferable in VANET.

In addition, no appropriate storage solution was offered on a real-time data



transmission scheme. The authors in [22] proposed a dynamic congestion control scheme (DCCS) for safety applications in vehicular ad hoc networks to determine only the network level security. The proposed scheme is a means whereby the reliable and timely delivery of data in safety applications can be ensured for road users and drivers. The proposed DCCS scheme objective also included the broadcasting of safety messages in order to ensure reliability and timely delivery of messages to all network neighbors. However, the disadvantage of the proposed scheme is that DCCS is without a fixed infrastructure. Moreover, there was no trustworthiness and efficient storage mechanism for the evaluation of real-time information in the network.

In [23], the authors proposed a location error resilient geographical routing (LER-GR) protocol for vehicular ad hoc networks to detect only the network level security. In the proposed LER-GR protocol, a Rayleigh distribution-based error calculation technique was utilized for evaluating error in location of neighbor vehicles. Based upon the LER-GR protocol, the least error location information was used for determining next forwarding vehicles. However, due to the dynamic mobility of VANET, the proposed protocol should have recommended an efficient storage solution and intelligence for data exchange in location information that would also ensure the reliability of data transmission.

Subsequently, there was no trustworthiness evaluation to assess vulnerabilities in the network for secure transmission of location data. In [24], the authors proposed an algorithm that achieved secured time stable Geocast (S-TSG) for VANET in a vehicular traffic environment for only the network level security. The proposed protocol was intended to detect vulnerabilities including DoS attacks in VANET, due to a decentralized, open

dynamic, as well as a limited bandwidth and control of overhead information. However, in the proposed protocol, there was no investigation conducted to evaluate either efficient storage or an intelligent and secure method solution in VANET for real-time data transmission. The protocol limitation also included an absence in optimize real-time vehicular traffic environment information processing.

In [25], the authors proposed a geometry-based localization for GPS outage in a vehicular cyber physical system (VCPS) (GeoLV) for network level security protection only. The proposed localization technique was a GPS assisted localization which has the tendency to reduce location aware neighbor constraints in cooperative localization. In addition, the proposed GeoLV utilized mathematical geometry for estimating vehicle location and focused on vehicular dynamics and the trajectory of the road. Based upon the proposed scheme, static and dynamic relocations were performed to reduce the impact of a GPS outage on location-based services.

However, the limitation of the proposed GeoLV technique was that it does not guarantee trustworthiness, and no FC method for efficient storage solution in VANET geometry-based localization for GPS outage in VCPS model was recommended or proposed in the scheme. It can be realized that the node level security detection was a major issue with the proposed schemes.

## **2.1 Securing VANETs-Fog Centric Distributed Architecture**

Security at the network level is defined as when the data has to travel from the source to the destination. Secured routing, key distribution, and the encryption of data

packets fall under the network security method. Fog computing is used to store the network data and to reuse it to accelerate network performance. In [26], the authors introduced fog computing to extend cloud computing in the context of the middle fog layer among cloud and mobile devices and produce various benefits. The authors utilized a key sharing mechanism for secure transmissions. In [27], the authors further discussed the usage of fog computing by using an event-based data gathering scheme.

When a data transfer is called in the network, a node is summoned to perform some activity, and an event occurs. A route discovery process contains 'n' events, including attaching hops from the source to the destination. The addition of a hop also requires the identification of trustworthy nodes, which utilizes optimization algorithms (OAs) to perform a successful operation to help solve this type of issue in computer science [28].

This research dissertation specifically utilized a hybrid of optimized Cuckoo search algorithms (CSA) [10], firefly algorithms, [15] and firefly neural algorithms [16] to investigate DoS and SNI attacks. The investigation also detected the node level and network level security and mitigated the attacks for trustworthiness in VANET. In [12], the authors also conducted an investigation about the cognitive behavior of VANET for high-speed mobility of VANET. In the investigation, it was discovered that VANET also experienced frequent topology changes. In addition, it was discovered that VANET incurred memory storage challenges for allocating spectrum resources. Hence, in [12], the authors proposed the improved adaptive binary Cuckoo search algorithm to investigate DoS attacks in VANET. The researchers in [15] used the firefly algorithm to investigate vehicles that travelled along highways which encountered some form of VANET attacks.

These vehicles that were deployed in the VANET were vulnerable due to DoS attacks which caused delays at the network level. Afterward, the authors utilized a clustering algorithm to facilitate good communication links. The authors' investigation centered on the real-time communication of the VANET to determine the efficiency of the messages for vehicles in order to receive traffic warnings in a timely manner. The authors' investigation conducted on the FA was also used to determine the reliability of the warning signals. The authors also conducted research in the FA and utilized the vehicles road-side infrastructure (RSU) regarding traffic safety warnings. In [16], the authors utilized the firefly neural algorithm, which is a combination of FA and a neural network, to investigate and train the VANET to determine the delay of the network. The parameters used for training the VANET were used to detect the network level DoS attacks, and the delay was evaluated in the network.

The firefly neural algorithm utilized a machine learning process studied in VANET to determine the misbehavior of the vehicles/nodes for detecting DoS attacks. The model consisted of four main phases including data acquisition, data sharing, analysis, and decision making. Hybrid OAs deployment including CSA, FA, and the firefly neural network, can integrate with fog computing and KDE to determine the node level and network level security against DoS and SNI attacks.

Hybrid OAs deployments select the best solutions or minimize unnecessary solutions to retain the contrast of the objective function. OAs are either heuristic or metaheuristic in nature. The heuristic approach has problem-solving skills but is not suitable for each domain. NP-hard problems fall under heuristic optimization algorithms. Non-

heuristic algorithms are adaptive in nature and may be applied for different sets of problems. More elaborately, the optimization can be further classified as Natural Computing, Swarm Intelligence, or Medical Computing. Both the CSA, FA and firefly neural network are classified as a Swarm Intelligence algorithms. There are various practices and architectures for the CSA, FA, and firefly neural swarm intelligence (SI) algorithms that relate to the CSA used in this research. In one practice or behavior, the Cuckoo bird lays its eggs in other birds' nest and leaves its eggs to be cared for by other bird species.

In another behavior, a Cuckoo destroys all of its eggs, even if only one egg is damaged, due to it considering that the eggs are not suitable for further reproduction. In addition, this research dissertation has utilized the second behavior of the CSA in combination with Lagrange's method and the other swarm intelligence algorithms such as FA and firefly neural network to select trustworthy nodes and ensure that the entire VANET is secure. The description is given in the subsequent section. The network may suffer from different kinds of intrusions or attacks. One of the most common security threats is the Denial of Service (DoS) and the SNI. In [29], different structures of DoS attacks that also address the concern of SNI are discussed and presented.

## **2.2 Securing VANETs-Centralized Architecture based on DoS**

### **Attacks and other related attacks**

In [30], the authors have proposed malicious nodes detection on vehicular Ad-hoc networks. They used Dumpster Shafer theory for investigating 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 for

investigating for real time detection of all forms of attacks including HDSA attack. Instead, the authors investigation was centered on only artificial neural network based technique, which used self-organized map. In the investigation also, the authors used only trace file to train the network that works as an input to self-organize map. This was in order to provide supervised learning to their network.

Although, the authors used SOM (self-organized map) classifier for detection of misbehavior nodes, the used method was not fully investigated and explained. Moreover, there was also limitation of utilization in IEEE 802.11 standard data transmission technique. The IEEE 802.11 would utilize the DSRC technology for investigating communications of vehicles in the network. This is observed as a major limitation of the scheme.

In [31], the authors have proposed prevention of DoS attack over Vehicular ad hoc network, using quick response table. However, based upon the proposed scheme, there was a limitation in the use of clear security method that was required for securing the network, which requires urgent attention. Another limitation observed with the scheme was that it did not conduct investigation regarding efficient storage mechanism for the network deployment. In addition, there was no recommendation for any trustworthiness method that would be used for securing the network. The detection of DoS attack was only based upon some form of attacks like gray hole, Sybil attack and black hole attacks only. However, these attacks are of different category.

Thus, the author's investigation could not be considered appropriate, due to absence in investigation in: DoS JSA, PD, and RCRCO overutilization, which relates mostly to the

trustworthiness and efficient data provision for RSU in VANET. However, it was discovered in the author's investigation that the proposed security mechanism was for merely discussing method for routing in VANET. 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 in VANET.

In [32], the authors have proposed an efficient and lightweight Intrusion detection mechanism for service-oriented vehicular networks (ELIDV). From the perspective of the authors, they have designed and implemented ELIDV with the aim to protect the network for only three kinds of attacks, including: DoS attacks, integrity target, 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 author's 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 attacks detection method used was not centered on any HDSA including: DoS JSA, PD and RCRCO overutilization. The proposed scheme was also identified with a limitation in designing a secure encryption/authentication mechanism. This would otherwise be used for providing a hybrid investigation of DoS attacks that would also include investigation in real-time data transmission in VANET.

In [33], the authors have proposed detection and prevention mechanism of

distributed denial of service (DDoS) attacks in VANETs. Based upon the proposed scheme, the authors concentrated only on DDoS attacks detection and the prevention scheme. The basic principle of the scheme relied only on keeping check on the number of packet 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 was limitation in the network which include, provision of any efficient storage mechanisms. This 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 limitation of trustworthiness in the network, CO was increased in the proposed scheme. Another limitation observed with the proposed scheme was 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 end2end delays in the network, which requires urgent attention.

The authors in [34] have proposed a review on IDS (Intrusion detection system). A survey on 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 with 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, 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 Honeypot optimized system. However, leading do the discussion of the authors proposed scheme, no investigation in network performance metrics evaluation of end2end delay, throughput and prediction accuracy performance of the proposed scheme were evaluated.

Based upon another limitation, which 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 investigated below based upon the concept in VFC.

### **2.3 Securing the VANETs-Fog Computing (VFC) Using Cloud Centric Architectures**

The authors in [35] have identified the security goals for VCC (Vehicular cloud computing; also known as VFC) interoperability. The authors have provided AKA (Authentication and Key Agreement) framework for VCC. Particularly, the authors proposed the problems with the challenges for the designing of consistent AKA with extra strong security assurance for VCC. 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 [36] introduced a novel method for serving speed-based lane changing, TOA (Time of arrival), 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 designing of TOA is for providing clear line of sights for exact services for localization and positioning applications. The authors have addressed collision avoidance with automatic braking and camera-based surveillance. The viability and feasibility of the algorithms have been established via simulation in SUMO (Simulation of Urban Mobility) and NS-2 (Network Simulator). The authors have designed a MAI (Mobile app interface) for the onboard unit for effective, smart with the monitoring of remote traffic.

The authors in [37] 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 have used varied cache discovery methods and examined the potential for addressing the appropriate challenges that occurred, while the deployment of non-safety application in VANET, which has avoided the common pitfalls. Future lies in the utilization of this research for the development of new co-operative caching methods like fog computing that could offer enhanced performance in VANET, while comparing the traditional approaches on the basis of co-operative caching methods.

The authors in [38] have 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 have introduced fog computing for the extension of cloud computing, with the context of middle fog layer among cloud and mobile devices for the production of varied benefits. As the keys are given directly from the middle layer, the latency is significantly diminished. Additionally, the amount of

messages exchanges among vehicles varied in VANET elements lessened, as compared to traditional methods. Accordingly, the resultant system is more effective. The design is executed and validated by network simulation tool for a single as well as the multi-vehicle system.

In [39], the authors have presented a novel technique for addressing the problem of data sharing and have delegated the data management to TPA (Trusted third party), on the basis of bilinear pairing method. For the achievement of this goal, the authors have utilized fog computing as the major tool for utility computing hypothesis for storing a large amount of data and have executed the re-encryption procedure safely. Varied resources like on board unit, communication, endless battery, computing is implanted in the vehicles for the usage for the enhancement of ITS (Intelligent transportation system) are used. 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 by revoking the traditional.

The authors in [40] used Firefly (genetic algorithm (FA)) to investigate vehicles that travelled along highways which 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 clustering algorithm to facilitate good communication links, however, VFC was a limitation for the network.

In [41], the authors have proposed a new unicast routing protocol for vehicular network. The protocol was based upon two techniques: clustering algorithm technique which played a purpose in organizing and optimizing exchange of routing information

based on quality of service requirement, and artificial bee colony Cuckoo (ABC) algorithm that 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/jitter in VANET is important.

The authors in [42] have proposed a scheme in Sybil attacks prevention, through identity symmetric encryption scheme in vehicular ad hoc networks. The author's investigation also includes DoS attacks and all forms of attacks including 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 in order to prevent malicious vehicles/nodes to obtain more than one identity inside the network.

The proposed scheme did not require management in RSUs or certification authority (CA). The scheme only utilized minimum amount of message exchange with the RSU, which according to the authors, they insist the scheme was effective. However, based upon the network deployment, some vehicles did not share information. Vehicles sends fake request and caused breakdown, leading to trustworthiness concerns in the network.

Based upon the work proposed in [43], which include "Early DoS Attacks Detection in VANET, it used Attacked packet Detection Algorithm (APDA)" for vehicles. The vehicle represents mobile nodes equipped with on-board unit (OBU) that allows them

to send and also receive messages from the other nodes in the VANET. The message successfully reached the intended destination without any interruption. In [44], the authors discussed DoS attacks in VANET and used the Bloom-filter- based detection method that provided service availability for legitimate vehicles/node in the network. Series of attacks were encountered in the network that caused communication break. This is due to DoS JSA, and source sink attacks and all the other forms of attacks including HDSA, which have been 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 methods 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 investigation of various proposed schemes in VANET complex to carry on. Also, it was determined in the investigation that VFC was a major design issue in VANET. Hybrid methods investigation deployment limitation persist. In addition, most of the proposed schemes investigation limitation revealed include trustworthiness concerns, secure storage mechanism and absence in hybrid optimization algorithms deployment that would be required for evaluating network performance metrics such as: end2end delay/jitter in the network.

Moreover, most of the schemes proposed by the authors which were based upon storage mechanism for processing information discussed focused on either using only unicast, multicast or broadcast method to assess VANET information processing performance metrics with the RSU. None of the proposed schemes had considered hybrid

unicast, multicast/broadcast and secure authentication/KDE deployments methods, for investigating all forms of attacks including HDSA. However, these limitations are major concern that would be required to be investigated further in VANET, in order to process safety and emergency message delivery in VANET. Thus, the authors of the above proposed schemes utilized insufficient end2end delay measurement methods, as discussed in sections 2.3 and 2.4 for VANET (VIA), for real-time detection in HDSA.

VANET optimization algorithm such as lion algorithm [2] was proposed in the literature to resolve routing concerns in VANET as subdivision of MANET (mobile ad hoc network). The algorithm/protocol was investigated to solve the route selection/discovery problem, which had an advantage of being deployed in large scale network. However, it was speculated that protocol general procedure used was not suitable for resolving the routing problem of the model. The protocol can also be investigated for limitation in fog computing and RSU processing of storage efficiency based on attacker influence in the network. In addition, the problem of trust resolution for attacks such as DoS and SNI is important. The protocol resolved congestion cost, collision cost and cost used QoS awareness cost.

However, investigation of these parameters based on attacker travelling cost within a specified transmission range would be necessary

# CHAPTER 3: DoS ATTACKS, INTRUSIONS AND PREVENTION MECHANISM IN VANET

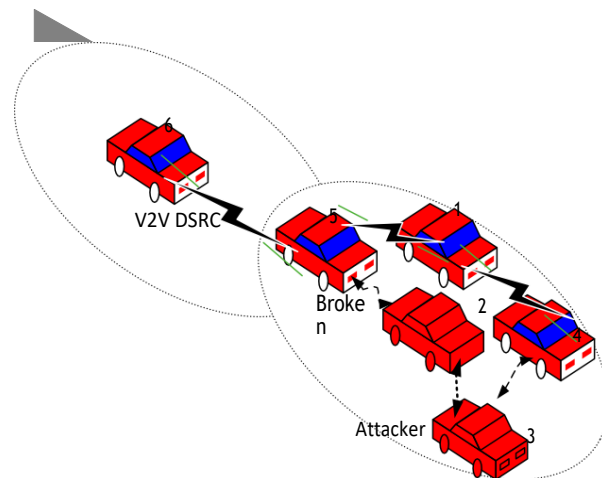
## 3.1 DoS Attacks

VANET experience DoS attacks [45]. These attacks intercept the channel at the data link layer. DoS attacks are capable of bringing down the available network resources. Through DoS attacks, the VANET can be exploited through the RSU due to the following:

- Resources consumption: DoS attacks consume the available network bandwidth. They inject fake routing messages, resulting in congestion over the VANET. This degrades the end communicating entities performance and introduces jitter.
- Signal jamming: DoS attacks have a high tendency to jam the transmissions while using channel interference.
- Packet Drops: DoS attacks have a high tendency to drop all or any selected packets. This interrupts the routing process from the source to the destination communicating entities.
- The investigation of VANET security provisions, such as certificate-based identification and an authentication mechanism are beyond the scope of this research.

### 3.2 Attack Principles

Unlike wired architectures where the channel blockage or congestion is always due to the increased flow rates at links with bottlenecks, congestion in a VANET may occur due to the aggregation property of the vehicles. If the attacker densely aggregates his attacks near the victim, the attacker can occupy more communication channels [46]. The total transmission capacity of one node increases a linearly with the increase in the area. If the node count does not vary, then the hop capacity is  $O(k)$ , where  $k$  is the node count of the network. The data transfer requires a route discovery, and the node count in a route may increase with the increase in the area. Each node has a probability of  $1/k$  of interacting with the channel. There are  $m$  nodes that can act as attacking nodes such that the victim node has the likelihood of  $(1 - m/k)$  of interacting with the channel. Figure 3.2 illustrates the channel occupancy and interaction of the proposed model architecture [47].



**Figure 3. 2** Channel occupancy.

VANET utilizes IEEE 802.11 as the most popular V2V DSRC (vehicle-to-vehicle dedicated short range communication) wireless system installed on almost every vehicle



where the vehicle/channel congestion/collusion are inevitable due to influence of the attacker vehicle encounter in the network, which could occur at the time when vehicles (or V2V) are required to transmit packets to each other in VANET. CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) is standard scheme that can be used to avoid such vehicle/channel packet transfer collision/congestion.

However, CSMA/CA is only a simple mechanism that can be used to allocate radio resources. In this research, we investigated how vehicle/channel occupancy can cause delayed packet transmission due to misbehavior of attacker vehicle which leads to broken link exposure of the vehicles communication process as shown in Figure 3.2. Figure 3.2 illustrates channel occupancy scenario based upon the attacker mode of operation.

In Figure 3.2 there are two types of vehicles, namely attacker vehicle and normal vehicle. All attacker vehicles have broken signals connections with each other. When attacker vehicle forms a connection with normal vehicle, a delay can be experienced in the network due to channel occupancy as a result of broken signal connection because both normal vehicles and attacker vehicles are in each other's communication range and the vehicles are traveling on the highway. The first ellipse from left to right has a transmission range (250 m), whereas the next ellipse has an interference range (550 m). Attacker 2 transfers packets to vehicle node 3, and this processes are highlighted in a broken V2V DSRC communicating signal, in which the packet is not received by another normal corresponding vehicle. Now, vehicle nodes 5 and 4 are in the range of vehicle node 3, but since it is occupied by attacker 2, it will have to wait, and an unnecessary delay will occur in the network. The channel occupancy vehicular attacker scenario is also used to illustrate

the misbehavior of compromised nodes in VANET due to DoS attacks [48].

### **3.3 DoS Attack Illustration**

A DoS attack employs multiple vehicles to attain its goal. It locks the job queue of the corresponding vehicle so that it is unable to accept data packet requests from genuine vehicles. Since a DoS attack is distributed over several vehicles, distinguishing authentic users becomes complicated. There are several ways to mitigate the effects of this type of attack, including encryption and the use of classification techniques. The use of authentication mechanisms can also be beneficial. Sanya Chaba et al. [8] presented a VANET architectural design for authentication key delivery with less delay between vehicles and with more mobility by utilizing fog and cloud computing. The authors have also introduced fog computing to extend cloud computing to the context of the middle fog layer among cloud and mobile devices for the production of various benefits. In their work, Qi Jian et al. [35] identified the security goals for VCC (vehicular cloud computing) interoperability. The authors have provided the AKA (Authentication and Key Agreement) framework for VCC. Notably, the authors have proposed the problems with the challenges for designing a consistent AKA with extra strong security assurance for VCC. A hybrid AKA framework has been suggested that combines the ‘single server 3-factor protocol’ with the ‘non-interactive identity-based key established protocol,’ which computes the performance by a simulated platform. Fog computing is utilized quite often these days for deployment of VANET, but its implementation has not been deployed with any KDE or key sharing for preventing SNI attacks, also utilizing the RSU.

Figure 3.1 illustrates an attack model scenario with the integration of the fog server

with vehicles. In Figure 3.2.1 RSU stands for roadside unit. The fog server keeps the information about the vehicles and distributes the required information to other vehicles if required. The intruder may also utilize same server and may misuse the server's information to spread false information [48].

### 3.4 Intrusion /Attacks Model

Figure 3.2.1 illustrates the intrusion /attacker model (IAM). The model detects and mitigates DoS and SNI attacks. The proposed IAM utilizes two types of vehicles; namely normal and intruder or collided vehicles. Normal vehicles are supposed to be on route. Normal vehicles denote all vehicles that have not experienced any form of attacks. Normal vehicles are the type of vehicles that are expected to arrive at their destination safely.

#### Legend

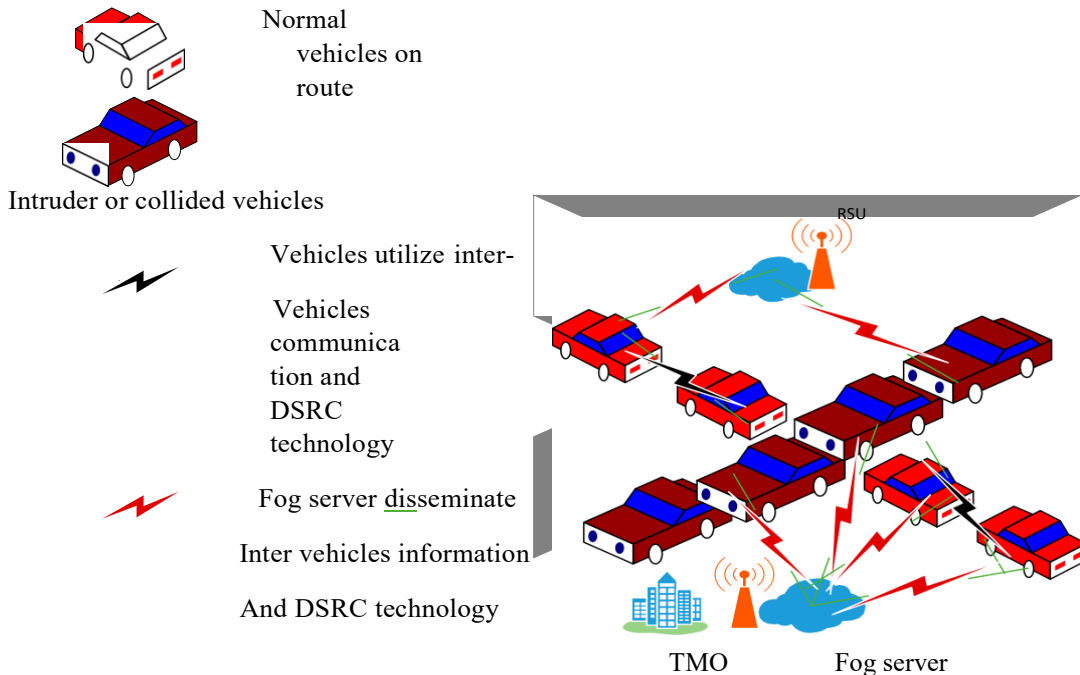


Fig 3.2.1 Intrusion Attacker Model

The intruder or collided vehicles, on the other hand, are the type of vehicles that have encountered intrusion attacks. Normally they are not expected to arrive to their destination. Moreover, the intruder vehicles have the tendency to introduce delays in the network. If intruder or collided/disabled vehicles are left unattended and continue to remain in the network, the network will suffer link breakdown and will not function as expected. This will lead to much delay encounter in the network. Delays of the network will lead to further road casualties since vehicles will not be appropriately informed. The proposed IAM initiates a remedy to prevent intruders/attackers in order to lessen road casualties. Therefore, in the proposed IAM, vehicles utilize antivehicle communication and DSRC technology. The vehicles communicate and share safety information with each other vehicle.

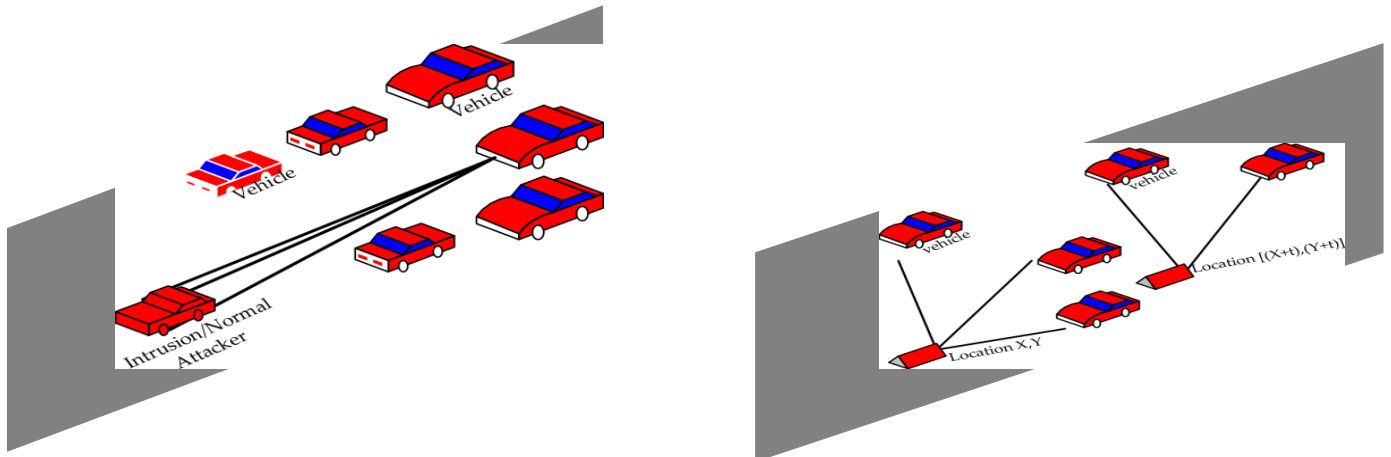
The information shared include condition of the vehicle and the road conditions. The information shared may also include congestion/collision and accidents that have already occurred. In addition, the fog server (FS) is deployed such that it addresses the location awareness concern in the cloud. The deployed FS disseminates emergency inter-vehicles information utilizing warning sign to alert other vehicles through the RSU information processing. The warning signal information can be obtained by each vehicle through the RSU and the FS which originates from the traffic management office (TMO). The TMO is the place where road safety applications (RSA) such including as SSVA, PCN, and CCA are deployed and connected with the RSU and the FS.

Two inter-vehicle communications, including the FS, utilize DSRC technology. DSRC technology is data link technology which utilizes the IEEE 802.11 standard for

transmitting information. Based upon this, real-time information, which convey warning and emergency information about any intruder activity in the network, can be received through the RSA. The network is also identified with the other forms of intruder/attacker such as smart and normal intrusion (SNI). SNI may sometimes go unnoticed and requires sophisticated approach to detect. Smart intrusions make the network feel like there is no threat in the network. If the intrusion follows a set pattern of dumping the packets, then it becomes easy to identify. However, the smart intrusions do not follow a consistent pattern [49]. The SNI scenarios that occur in the VANET are depicted as in the figures below

### 3.4.1. Smart and Normal Intrusion/Attacks Scenario

Figure 3.4.1a, 3.4.1b represents the normal and smart intrusions (SNI) attacker scenarios. The proposed IAM relies on the SNI intensity to evaluate the delay of the network. The intensity and location of the normal intrusion does not change with the change in the time frame, whereas smart intrusion changes the location and intensity of the attacks with



**Figure 3. 4.1 (a)** Normal intrusion/attacker;

**3.4.1 (b)** Smart intrusion/attacker.

Every instance. As shown in Figure 3b, the Intrusion is at location  $(x, y)$  at time  $t = 0$ , and it instantly changes its position at time  $t = 1$  and goes to  $(x + t)$  and  $(y + t)$ . The

intrusion even changes the location and intensity of the attack at every instance [50]. The SIVNFC system architecture prevention mechanism (SAPM) is a sophisticated approach that can be utilized to determine and mitigate the SNI attacker in the VANET as demonstrated below.

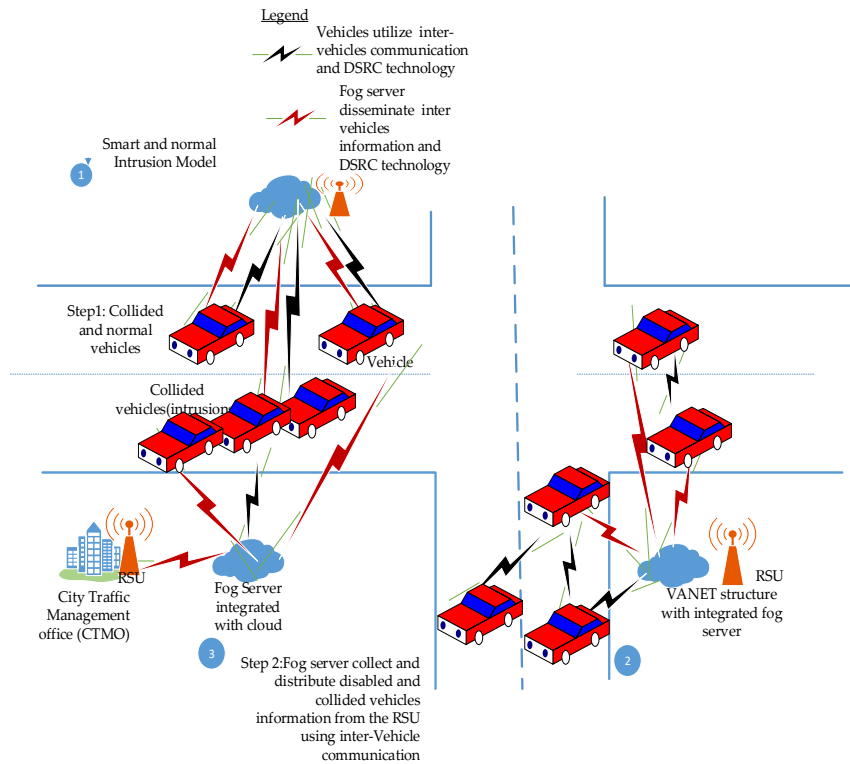
## **CHAPTER 4: MATHEMATICAL MODEL AND IMPLEMENTATION**

### **4.1. Proposed System Architecture Prevention Model (SAPM)**

Figure 4.1 depicts the proposed SAPM. In SAPM, vehicles utilize two DSRC technology instances for information transmission (the DSRC technology uses the IEEE 802.11 standard for transmitting information). In one instance of information transmission, vehicles communicate among themselves using intervehicle or V2V communication. In the other instance, the FS forms a connection with the RSU and, through this arrangement, disseminates inter-vehicle information to all vehicles in the network. The information conveyed usually include collusion/congestion, intruder activity of the network such as SNI of vehicles, or information of vehicles that have encountered attacks. The disseminated vehicle information may also include reporting the state of vehicles conditions and the road conditions that are threatening.

The proposed SAPM also employs further preventive measures to detect and mitigate all forms of attacks, including DoS attacks that may go unnoticed. Some of these attacks include but are not limited to packet drop, jamming of channels, and the RSU resources consumption overutilization. Two models are deployed in the SAPM, namely IAM and VANET structure with integrated for server (VSIF) models. The models utilize steps and scenarios for prevention and protection of the network against DoS and SNI

attacks. In step 1, collided/disabled vehicles or intruder activity are detected and reported to the other vehicles in the network utilizing the IAM. The IAM detection of intruder/attacker has already been explained in detail above. In scenario 2, the VSIF model is deployed. The deployment of the VSIF model is also illustrated in Figure 5. The VSIF model relates and connect with the proposed SAPM as below.



**Figure 4.1** Proposed Secure Intelligent Vehicular Network using Fog Computing (SIVNFC) system architecture prevention model.

The VSIF model deployment in SAPM includes the RSU connection with the FS Step 3. Scenario 3 (Figure 4) illustrates the deployment of VSIF model, the FS, and the RSU connection. FS collects intruder or collided vehicles or any unusual network attack information. The FS also obtains information concerning all forms of DoS and SNI attacks that may be eminent in the network through the RSA which is installed at the TMO. The



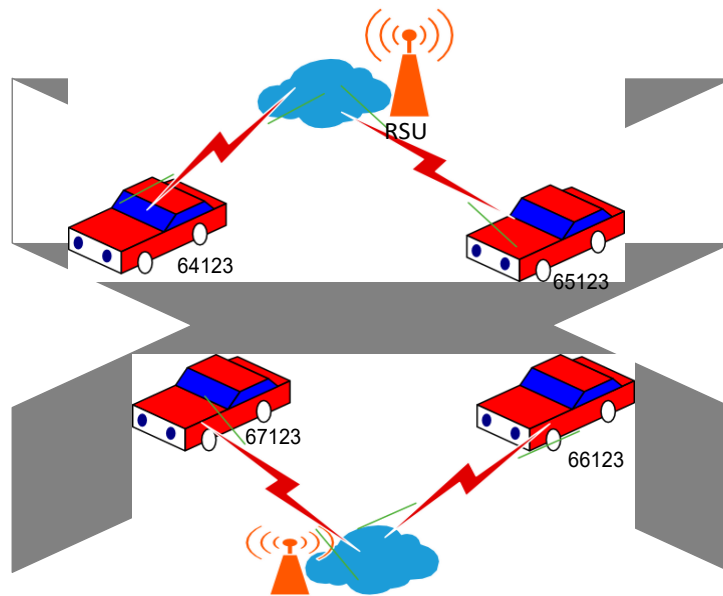
TMO is presumed connected with the RSU. The VSIF model utilizes inter-vehicle communications connections based upon the following deployment explanations.

RSU (Roadside unit): RSUs are gateways. Gateways are also deployed in the proposed SAPM which establishes connections with the FS. The RSU is equipped with network devices. It utilizes DSRC inter-vehicle communication packet transfer based on IEEE 802.11. RSU to FS: VANET utilizes V2V and V2RSU communication to propagate safety/non-safety information. RSUs communicate with each other as well. Thus, RSU behaves as the FS backbone. Wireless and wired connections are formed between RSU and FS (Figure 4.1). The RSU is aligned with FS.

Fog Server to Fog Server (FS to FS): FSs are identified at different locations. They interact with each other. Consequently, a pool of VANET resources that is localized can be managed through the TMO. This connection can be achieved via vehicular control center traffic management or TMO, as shown in Figure 4.1. Thus, direct wireless and wired communication between peer FS can be possible. In addition, collaborative services provision and the FS peer contents delivery can be initiated at the TMO, which improves the entire SAPM. In addition, the cloud is logically connected with the FS and has the tendency to aggregate information.

Fog Server to Cloud: In the proposed SAPM, FSs utilize fog computing to address location awareness concern of cloud computing. Thus, cloud computing represents a central portal of information which does not require location awareness for information processing. The cloud centrally controls the FS in various locations. A FS possesses the capability to aggregate the information that it has obtained from other FSs. The VSIF

utilizes centralized computations whereby FS transmit intervehicle information that it has received from the cloud to the application users [51], utilizing the DSRC technology. Due to open nature of the VANET deployment and associated vulnerabilities, RSU and the FS utilize an authentication/KDE preventive mechanism in the proposed SAPM for ensuring real-time packet delivery



**Figure 4.1.1** VANET (vehicular ad hoc network) structure with Integrated Fog Server Model.

The proposed SAPM utilizes two levels of authentication/KDE preventive mechanisms for the FS and the RSU aggregation of information, namely. The RSU-L considers the vehicle's displacement and jitter in the VANET, whereas the FS-L utilizes the Lagrange Polynomial for the identification of untrusted nodes as well which also utilize DDoS architecture as below [52].

### 4.2 DDoS SAPM

The distributed DoS (DDoS) attack includes all the DoS attack and the SNI (Smart and normal intrusion) attacks in the model. These attacks mitigation approach in the model utilizes multicast broadcast and unicast data in the network. This scatters the attack traffic throughout the network distributed fog server in connection with the RSU, to the point where the network traffic could completely be absorbed. Multicast broadcast and unicast data reliability that can be used to mitigate the DDoS attack depends on the attacks size and the network efficiency size. The Fog server and the RSU is implemented to mitigate a vital part of the DDoS attacks. This uses the multicast broadcast and the unicast data to mitigate the attacks, utilizing the specialized designed network equipment using the cloud-based fog computing and the RSU protection services, a targeted victim mitigates any incoming DoS and SNI incoming attacks.

The DDoS attacks encompass DoS and SNI attacks stages Mitigation are as follows:

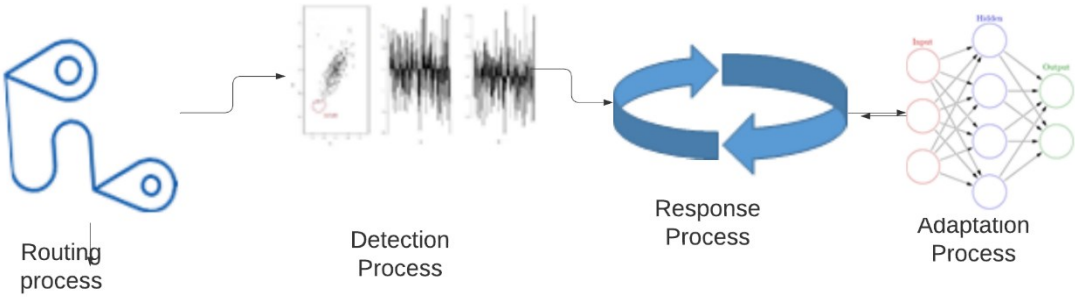


Fig. 4.2 DDoS Attacks and SNI Attacks Stages Mitigation

### 4.3 Fog Server-Level(FS-L) Prevention Mechanism

The FS-L keeps one global key for the entire network; hence, each vehicle is identified by the global key itself. Distributing the global key in the vehicles is insecure; therefore, the vehicles follow a shared system. Each vehicle has its own shared value.

When a vehicle requests the information from a server either directly or through an RSU, the fog server will demand three shares from any vehicle in the network or will choose two of them randomly [53]. Three total shares will be considered, including the demanding vehicle. The fog server will utilize the Lagrange polynomial to calculate the following.

The Lagrange polynomial  $S(X)$  containing degree  $\leq (n - 1)$  demands  $x_1, y_1 = f(x_1)$ ,  $x_2, y_2 = f(x_2)$ , ...,  $x_n, y_n = f(x_n)$  is given by:  
 $n$  vehicles with coordinates  $(x_1, y_1 = f(x_1)), (x_2, y_2 = f(x_2)), \dots \dots (x_n, y_n = f(x_n))$  is given by:

$$S(X) = \sum_{k=0}^n P_k(X) \tag{1}$$

Where  $P_k$  is given by

$$P_k(X) = y_k \frac{x - x_l}{x_j - x_l} \text{ where } 1 \geq 1, l \leq n \text{ and } l \neq k \tag{2}$$

If written explicitly for  $n=3$  vehicles,

$$S(X) = \frac{(x - x_2)(x - x_3)}{(x_1 - x_2)(x_1 - x_3)}y_1 + \frac{(x - x_1)(x - x_3)}{(x_2 - x_1)(x_2 - x_3)}y_2 + \frac{(x - x_1)(x - x_2)}{(x_3 - x_1)(x_3 - x_2)}y_3 \quad (3)$$

The separate polynomial can also be formulated as with Szeto (1975), which was later called Lagrange's fundamental interpolation.

$$S(X_1) = \frac{x_2 * x_3}{(x - x_2)(x - x_3)}y_1 \text{ for the first vehicle} \quad (4)$$

$$S(X_2) = \frac{x_1 * x_3}{(x - x_1)(x - x_3)}y_2 \text{ for the second vehicle} \quad (5)$$

$$S(X_3) = \frac{x_1 * x_2}{(x - x_2)(x - x_3)}y_3 \text{ for the third vehicle} \quad (6)$$

The key that is generated by the integration of separate polynomials is represented as

$$G_k = \sum_{k=0}^n S(k) \quad (7)$$

If  $G_k$  matches the network key, only then does the vehicle pass any information from the fog server. Second, the FS level security is also applied, which makes the network more secure. To understand the structure of this security, the pseudo code is also given as follows.

---

**Algorithm 4: Pseudo Code Algorithm for Share Verification**

---

**Notations:**

*SODFSV*: Shares Ordering Demanded by FS from Vehicles:

$ISVM_{y_{VALUE}}[]$ : Initial Share for Vehicle Value being Empty

$SCV$ : Share for Current Vehicles

$SKV$ : Share Key Value

$SVCV$ : Share Vehicle Current value

$V_i$  : Individual  $i^{th}$  Number of Share for Vehicle

$ICNSV$ : Initial Counter Number for Share of Vehicle

$CSVBI$ : Current Share for Vehicle/Node Begin Iteration

$SVNID$ : 1<sup>st</sup> Share Key Vehicle/Node Identification or Initial Reference

$SVNID_{Num}$ : Share Numerator key for Vehicle/Node Identification in Network

$SVNID_{Deno}$ : Share Denominator key for Vehicle/Node Identification in Network

$V_j$  : Individual  $j^{th}$  Vehicle Chosen for Share in next Iteration

$SV_jC$  : When first Vehicle Share is Chosen there will be 2 remaining Share for the Vehicle

$SVCNS$ : Share for Vehicle Chosen Current no same as next Share Chosen

$RSCV$ : Remaining Share Counter for Current Vehicle

**Input:**  $S(k), n, i, k, j,$

**Process: Initialization**

$V_i = V_j;$

$ISVM_{y_{VALUE}}[] = \emptyset;$

$SODFSV=2;$

$SVNID_{Deno} = \emptyset;$

1. **If**  $ISVM_{y_{VALUE}}! = \emptyset;$

2. **for**  $V_i = 1: 3$

**While**  $ICNSV = 1;$  **then**

a.  $CSVBI = SVNID;$

b. **for**  $V_j == 1;$

c.  $CSVBI = V_j;$

- d. **If**  $CSVBI \neq V_j$ .
- e.  $RSCV = SV_jC$  ;
3.  $RSCV = RSCV + 1$ ;
4. **End if**
5. **End for**
8.  $SVNID_{Deno} = V_j - (RSCV * V_j) - SV_jC$
9.  $SVNID_{Num} = RSCV * SV_jC$
10.  $ISVM_{MyVALUE}[i] = \frac{SVNID_{Deno}}{SVNID_{Num}}$
11.  $SKV = SV_jC * ISVM_{MyVALUE}[i]$
12. **End for**

**Output:**  $G_k, SCV$

---

The pseudo code uses the interpolation order [54] of two and only three nodes for communication. Whether the nodes will be selected for the data communication or not depends upon the final key result, which is calculated using Lagrange's method. One key generation method requires a numerator and a denominator. The numerator is calculated using network IDs of the vehicles that remain for the iteration [55]. For example, we consider 45, 53, and 61 to be the nodes that are selected for the verification. Therefore, the numerator value (Num) for 45 is  $53 * 61 = 3,233$ . the denominator (deno) is calculated by multiplying the difference of the network IDs of the remaining nodes. For 45, the deno value will be  $(45 - 53) * (45 - 61) \rightarrow (-8) * (-16) \rightarrow 128$ . The verification key would be the product of the Shared key of 45 to  $\frac{Num}{Deno}$ . Similarly, the Shared<sub>key</sub> for 53 and 61 will be calculated. The final verification key would be the sum of all the generated verification keys.

$$\text{Final}_{\text{key}} = \sum_{k=0}^i \text{My}_{\text{value}} \quad (8)$$

If the  $\text{Final}_{\text{key}}$  is equal to the network security key, then the nodes are selected for communication. Lagrange's theorem randomly selects the nodes for verification. Though the verification process of Lagrange is good enough, to make it more efficient, the CSA is applied to select the nodes for which the verification keys will be generated. The CSA uses the node distance and its feedback to judge whether it should be considered for key generation or not. The final verification key would be the sum of all the generated verification keys.

Table 4: Specifications Considered for the Cuckoo Search Algorithm (CSA).

<b>CSA Population</b>	<b>Total Nodes in Coverage Region of Demanding Node</b>
Fitness Parameters	Feedback, Location Difference (LD)

$$\text{LD} = \sqrt{((x_{nx1} - x_{nx2})^2 + (y_{ny1} - y_{ny2})^2)} \quad (9)$$

LD is the location difference between the demanding node and the communicating node.

The CSA fetches the feedback values of nodes from the fog server, which also obtains intervehicle information through the RSU.

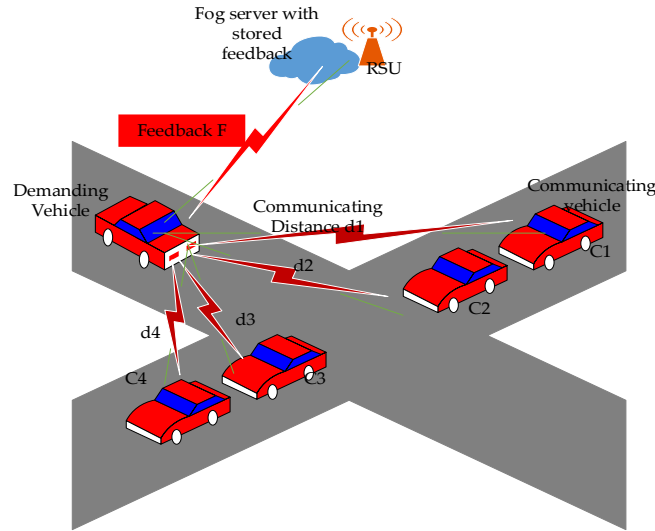
As shown in Figure 4.3, the main node computes the distance between the demanding node and the communicating node. It fetches the feedback from the fog server through the RSU and utilizes it for the fitness function.



$$\text{If Fitness}_{\text{function}} \rightarrow \text{Return 1 if } \frac{d}{f} < \frac{\sum_{k=0}^n \frac{d_k}{f_k}}{n} \quad (10)$$

Return 0 otherwise

where  $d$  is the distance between the fog and the user and  $f$  is the feedback of the fog server.



**Figure 4.3.** Node Communication with Fog server.

The data transfer will take place once the route discovery (RD) process is complete which uses the RD communication cost model as below.

#### 4.4 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 which denotes VFC can store a lot of data which can be reused and can be aggregated to prevent time successions search, as the vehicles do have much onboard storage [38].

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 to know that packets are either received effectively or not. When the vehicles in the cloud have the data packets, then vehicles verify to know 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 state election mode. Later, vehicles unicast the received packets towards the parent cloud to send the packet till packets arrive at the cloud leader which discloses about the vehicle information. Accordingly, as shown in the below algorithms, if the cloud leader produces a data packet, initially it verifies about the packet source.

When the data packet approaches from enode-B (an element of LTE (long term evolution) 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 LTE data packet ( $LTE_{dp}$ ); which transfer the packets to the enode-B with the novel original received packet from the vehicle. In the end, the packets are updated as CLvInf (Cloud leader vehicle information). The PSAM utilizes the multicast/broadcast and unicast modelling in order to fulfill the requirement as per need. Obviously, the multicast architecture incurs some

latency and as it broadcast the data, it will consume some time.

#### **4.5 Communication Cost Model**

In this model, VANET optimization algorithm LAC (lion algorithm cost) denoting CSA optimization algorithm [64] is investigated as subdivision of MANET. It is developed as minimized routing cost under VANET and has been modified in the proposed SIVNFC scheme under CSA optimization algorithm. The LCA algorithm transmission range for communication is an issue[64]. In addition, the algorithm has limitation in trust provision due to DoS, and SNI attacks concern posing serious security threats.

Moreover, there are issues like improved storage, and fog computation solution for VANET condition that require enhancing the jittering/delay and prediction accuracy for the proposed SIVNFC scheme for efficient road safety application. With improved storage and FS computations, trust concerns due to DoS and SNI including channel occupancy, can be optimized through the proposed SIVNFC scheme, utilizing the CSA optimization algorithm determination in VANET. In this dissertation, CSA is utilized as the optimization algorithm for the proposed scheme that adopts the method of modified routing cost, for route discovery (RD) in VANET. Through this, the estimation of attacker congestion cost, attacker collision cost, channel occupancy by attacker travel (CCT) cost and QoS awareness cost, can be discovered and estimated in VANET.

This also helps to determine the less jitter and improved throughput performance of the proposed SIVNFC scheme.

DoS and SNI in the network lead to computation in route discovery (RD) cost. This would be necessary and given as  $i = RD_{i,j}$  where  $i = 1, 2 \dots V^{attacker\ path}$  and  $j = 1, 2 \dots V^{nodes}$ . This is such that  $(RD)_{i,j} \in \{LD\}$  and  $V^{attacker\ path}$ , where,  $LD$  represents vehicles various location difference within a specified transmission range in the network, during a given period.

This should be equal to  $M^{vehicles}$ , where  $M^{vehicles}$  denote the number of vehicles in the network, where the concerned vehicles ( $j^{th}$  vehicle) is denoted as  $V_j$   $j = 1, \dots M^{vehicles}$  and  $RSUFS_n$   $n = 1, 2 \dots k_{RSUFS}$ . Generally, Paths of travel of each vehicle correspond to all path of smart and normal intruder vehicles activities in the network that requires determination. Consequently, the precise RD cost of the network can be determined as shown in Eqn. (1) below:

$$C_{ost}(RD) = C_{ost}^{congestion\ by\ attacker} + C_{ost}^{colliision\ by\ attacker} + C_{ost}^{channel\ ocupied\ by\ attacker\ traveling} + C_{ost}^{QoS} \quad (1)$$

Where,  $C_{ost}^{congestion\ by\ attacker}$  is congestion cost due to an attacker in the network,

$C_{ost}^{colliision\ by\ attacker}$  collision cost due to an attacker,

$C_{ost}^{channel\ ocupied\ by\ attacker\ travelling}$  is cost of channel occupancy by attacker travelling

in a given transmission range and  $C_{ost}^{QoS}$  refers to QoS awareness cost

The congestion cost due to an attacker can be estimated through identifying all intruder/attacker vehicles that can obtain information from the  $RSUFS$  (i.e. RSU and the fog server (FS)), including the tendency to compromise the integrity of the data, during a

given duration of vehicle travel. In equation (3), below  $C_k^{attacker\ limit}$  indicates congestion due to attacker limit of  $k^{th}$  RSUFS, and this is referred to as the maximum capacity, in which the RSUFS can be used for handling any attacker compromised traffic.

Thus, equations below are estimated *for*:

$C_{ost}^{congestion\ by\ attacker}$

,  $C_{ost}^{colliision\ by\ attacker}$ ,  $C_{ost}^{channel\ ocupied\ by\ attacker\ travel}$  and  $C_{ost}^{QoS}$

as follows:

$$C_{ost}^{congestion\ by\ attacker}(j) = \begin{cases} C_k^{over}(j), & C_k^{over} > 0 \\ 0, & otherwise \end{cases} \quad (2)$$

$$C_{ost}^{QoS}(j) = \sum_{\substack{i=1 \\ j \neq 1}}^{V_{attacker\ path}} CS_k(i, j) - C_k^{attacker\ limit} \quad (3)$$

$$CS_k(i, j) = \begin{cases} 1, & if (RD)_{i,j} \in C_k \\ 0, & otherwise \end{cases} \quad (4)$$

The overall total cost involved for the vehicles to communicate within an effective transmission range and deliver road safety information to each other is referred to as the effective traveling cost for avoiding attackers'/intruder capability in the network.

The  $C_{ost}^{channel\ ocupied\ by\ attacker\ travel}$  is determined based on equation (5)

$$C_{ost}^{channel\ ocupied\ by\ attacker\ traveling} = \sum_{i=1}^{V_{attacker\ path}} \sum_{j=j+1}^{V_{attcker}} (LD) ((RD)_{i,j-1}, (RD)_{i,j}) \quad (6)$$

Where LD as obtained in the CSA optimization algorithm

Similarly,  $C_{ost}^{QoS}$  is determined for QoS awareness in the network using fuzzy inferences system [2,3]. The attacker congestion level of RSUFS can be determined based on the cost validated, using the fuzzy inference system [2, 3]. The attacker total collision probability cost can be determined using similar manner as shown in the collision algorithm in [2].

QoS Cost Model Analysis Graph

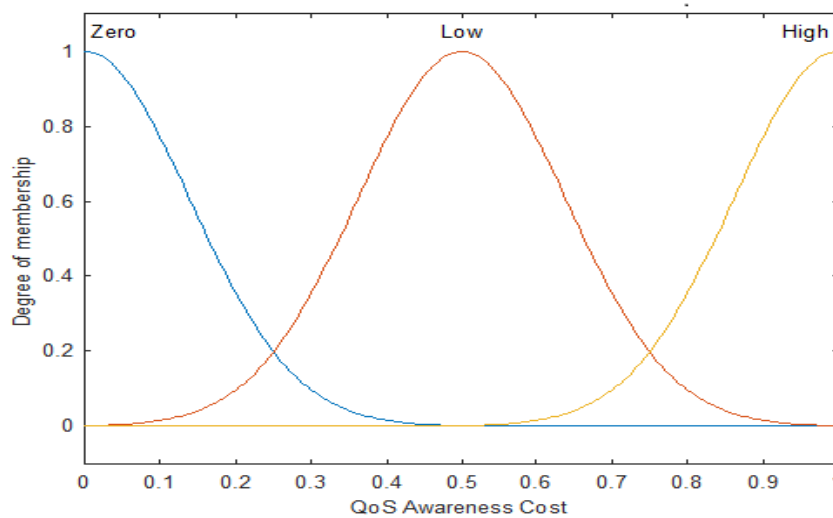


Figure 4.5 Degree of membership Vs QoS Awareness Cost

QoS awareness cost can be estimated based upon simulation parameters used. It includes using factors such as the received signal strength (RSS) that determine delivery of efficient RSA and, based upon fuzzy logic system [98]. It may also include non-numeric linguistic variables (NLV). Generally, numeric values are given to the above mentioned NLV. They are used as a member function of the fuzzy logic system. Fuzzy rules, required for determination of the QoS factors and cost include QoS awareness cost which could be: zero, low and high as shown in above figure 7. A high QoS awareness denote higher RSS for the proposed scheme that can deliver efficient driver safety information on the road.

A network also suffers from two kinds of security issues—namely, the node level and

the data level. This paper further addresses the node level security [56].

#### 4.6 Node Level Security

VANET is a type of ad hoc network whose survival depends on vehicle/nodes cooperation and trust. Therefore, trust between vehicles requires enforcement. Trust models can be categorized into vehicle/node trust or data trust.

With node level trust security, vehicles/nodes evaluate trustworthiness between them, whereby each vehicle crosschecks their neighbors redundant sensing data with their results. Trust in vehicles can be calculated through a lightweight method and data which includes three parameters: Sensing a data consistency value (or throughput), VANET communication ability, and the Vehicle/nodes remaining lifetime. Trust assertion makes inconsistent data from DoS and SNI attacks to be detected [57].

The node level security is achieved by calculating the trust of neighboring nodes. The calculated trust values are stored in the fog server for further processing.

The mathematical equation for node level security in the VANET is calculated by determining the trust values of the node which is given as:

$$B = \bar{\tau} \sum_{i=1}^n N_{xi}(Y) \quad (11)$$

The above equation shows that there is  $n$  number of trust factors.  $N(Y)$  indicates the trust value of the node of  $i$ th category. It is seen that if  $B$  is greater than or equal to  $N$ , the associated risk is less than threshold value and then node  $x$  will do work for  $Y$ . Node

X keeps on checking to see any recommendations about Y node from neighboring nodes, and, if so, the trust value is calculated using the following equation.

$$C = \frac{\sum_{x=1}^z N_x(Y)}{z} \quad (12)$$

where z indicates number of neighboring nodes and  $N_x(Y)$  indicates the trust value of node X on node Y. The vehicles that have been identified as trusted nodes interact with the RSUs through the FS to obtain the data in the appropriate order [58]. The proposed SIVNFC scheme utilizes an RSU prevention mechanism whose model is as follows.

#### 4.7 RSU-L Prevention Mechanism

The network deployment is based upon the specifications in Table 4.7.

**Table 4.7.** Network Specifications.

<b>Total Number of Vehicles</b>	<b>50–100</b>
Height of the Network	1000 m
Width of the Network	1000 m
Node Displacement	100–500 m/s
Simulation Iterations	1000
Simulation Tool	MATLAB

---

#### Algorithm 4.7:Pseudo Code for Vehicle Placement

---

// To maintain the randomness in the network, the network is set in a random manner

1. For each n Nodes
    - 1.1.Xloc(n)=1000\*rand// Create a random x coordinate
    - 1.2.Yloc(n)=1000\*rand
    - 1.3.Place(Xloc(n),Yloc(n))// Place the node in the network
  2. End For
-



Vehicles have different sets of parameters. The functions are designed to initiate the network parameters. A real-time simulation may result in different structures. In addition, a network may not include any fixed structure; however, for the sake of any simulation, some parameters should be initialized.

---

Algorithm 4.7.1: Pseudo Code to Initialize Vehicle Features

---

1. For  $i=1:\text{Nodes}$  // Loop running for each node
    - a.  $\text{Delay}_n(i)=\text{Random } D$ ; // Include a delay value if the node is acting normally
    - b.  $\text{Delay}_t(i)=\text{Dealy}_n^2$ ; // For now, the expected reality is unpredictable; hence, just the random //architecture is it set to be the square of the normal delay
  2. End for
- 

Vehicles have different sets of parameters. The functions are designed to initiate the network parameters. A real-time simulation may result in different structures. In addition, a network may not include any fixed structure; however, for the sake of any simulation, some parameters should be initialized. As the delay is initialized in a similar fashion, the other network parameters such as the jitter and packet drop are also initialized. The battery consumption is not a problem in the case of a VANET since the battery continues charging as long as the vehicle is running [59].

Figure 4.5 (a), 4.5 (b) represents the path construction and attack mode of the attacker. Figure 4.7b shows that the intensity of the attacker varies at different times. If the intensity is high, the attacker is attempting to dump more packets. The above attacker scenario is demonstrated in the equations below.

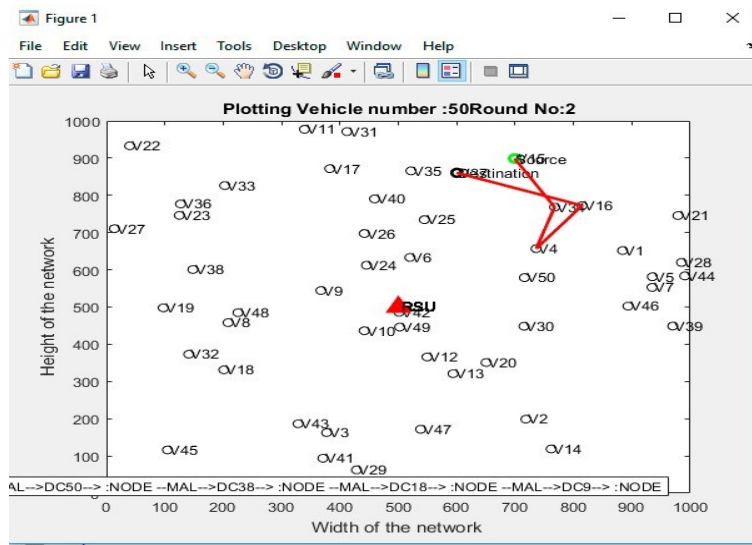
$$T_{pd} = P_{dn} + P_{da} \quad (13)$$

where  $T_{pd}$  is the total packet drop,  $P_{dn}$  is the total number of dropped packets in the normal

mode, and Pda is the dropped packets when the network is threatened.

$$Pdr = \frac{T_p - T_{pd}}{T_p} \quad (14)$$

where Pdr is the packet delivery ratio, and T<sub>p</sub> is the total number of packets. The random behavior of attack makes the network architecture more sophisticated. Now, challenge is



4.7(a) Constructed Vehicle Path.

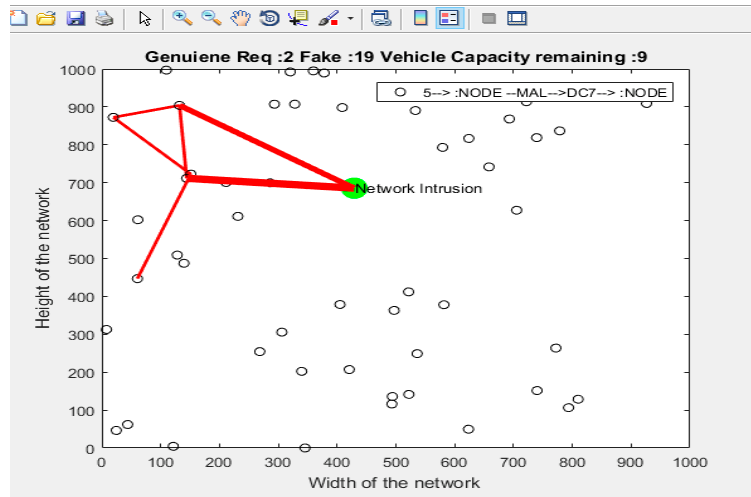


Figure 4.7. (b) Attacker Path

to identify them. The proposed solution utilizes the feedforward back propagation neural

network (FFBP-NN), and the general utilities of the FFBP-NN are given in Table 4.7

**Table 4.7.1** Utilized Feedforward Back Propagation Neural Network (FFBP-NN)

Total Hidden Layer	1
Neuron Counts	30
Feeding Iterations	100
Reverse Iterations	40-60
Propagation Type	Linear
Algebraic Model	Levenberg

The Artificial Intelligence (AI) method is made up of two sections:

- Training and Classification

The classification section is used in the identification model. The training module utilizes the jitter as the training parameter. To train the neural network, the neural network toolbox in MATLAB is utilized. The training layer is provided with the target set as well. The target is the identification of the nodes. The training consists of two phases. First, training is performed for the identification of the path, and then the training is performed for the identification of the affected vehicle(s) in the route [60].

The following equation can be defined:

$$J_{tr} = D_p(a, n) + N_d \quad (15)$$

where  $J_{tr}$  is the jitter,  $D_p$  is the delay of the path, and ‘a’ and ‘n’ represent the advanced (under threat) and normal situations, respectively.  $N_d$  is the network delay. For each path in every iteration, there will be jitter. The proposed solution uses the first 400 iterations’

data for training and then uses the next 600 iterations' data with the training.

---

Algorithm 4.7.2: Algo Train\_Neural (Iteration\_Data, Total\_Iterations)

---

For i=1:Total\_Iterations

    Training Data (i) =Iteration Data (i); Targetable (i) =Path ID;

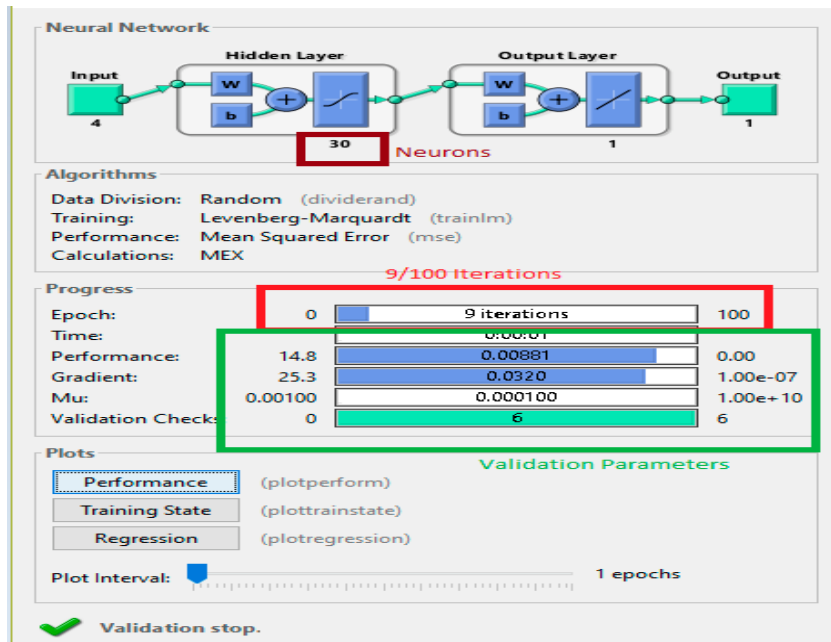
End For

    Neural=Initialize Neural (Training Data, Target Label, k); // k→ Total Neurons (30 in this case)  
    NeuralI.TrainParam.Epochs=100; // Total training iterations

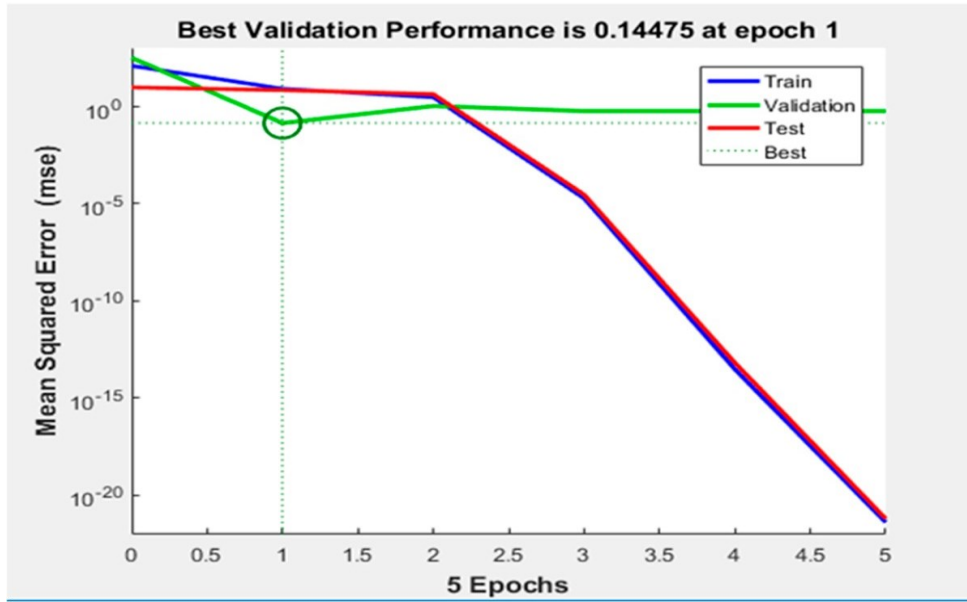
    Train (NeuralI.Training\_Data, Target\_Label); // Training with Initialized Neural and Training data  
End Algorithm

---

The training section results in FFBP-NN structure given in Figure 4.7.1 a and b



4.7.1 (a) Feed Forward Structure.



4.7.1 (b) Back Propagation Firefly.

## 4.8 Identification of Affected Node(s) and Recovery

The proposed research work also presents a regression model with backpropagation.

Figure 4.8 represents the regression model and values.

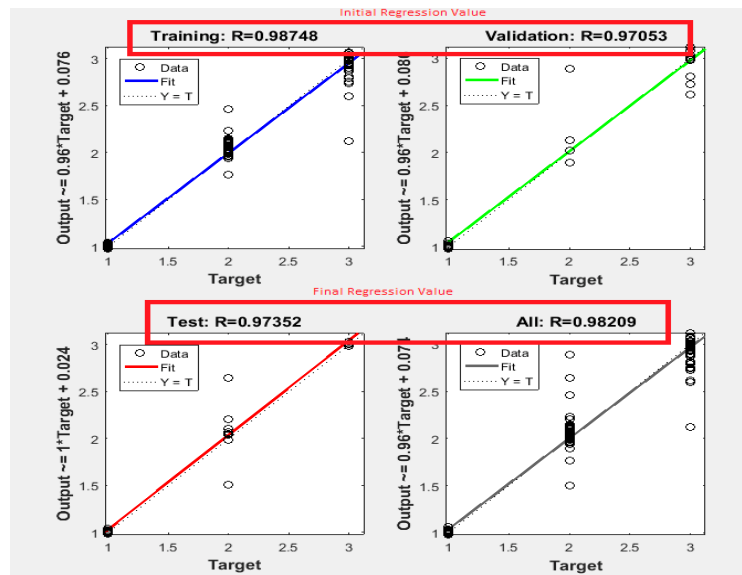


Figure 4.8 Regression model

## **CHAPTER 5: RESULTS, ANALYSIS. AND DISCUSSION**

### **5.1 Feed Forward–Backward Propagation and Regression Model**

#### **Result and Analysis**

##### **5.1.1 Feed Forward–Backward Propagation**

From Figure 4.7.1(a) and (b), we can see that the proposed scheme calculates both the training data for latency (jitter) and validation of jitter that is the deviation between the predicted  $y$  and the actual  $y$  as a measure by the mean squared error (MSE). We can see that we have five Epochs for our model. This means that we are essentially training our model over five forwards and backwards. The five epoch is also the stopping iteration and the one epoch for back iteration. The expectation is that the proposed SIVNFC scheme will decrease with each epoch, which means that our model is predicting the value of  $y$  more accurately as we continue to train the model.

The predictions of the test data show how good the proposed SIVNFC scheme is. The test graph in Figure 4.7.1(b), which indicates validation performance at epoch 1 of the model, indicates our model predictions is a good one.

From the graph in Figure 4.7.1(b), we can see that both the training and the validation loss decreases in exponential fashion as the number of epochs is increased. This suggests that

the model has gained high degree of accuracy as our epochs (i.e., the number of forward and backward passes) is increased.

### **5.1.2 Regression Model Result and Analysis**

Figure 4.8 represents the close and high regression value of the proposed scheme. The result indicates that the proposed model close and high regression values are: Training is 0.98748, validation is 0.97053, test is 0.97357, and the value for all is 0.98209. All these regression values are close and high as well. Close and high regression values generally represent healthy training and classification structure. High regression value is the reason because of which the prevention parameters are high for the proposed model to prevent much jitter/delays in the SAPM architecture.

As discussed earlier, this section classifies the path value on the basis of the trained structure. The identified attacker nodes are always sent for recovery or maintenance.

## **5.2 QoS Provision Analysis in VANET**

Development of VANET has recently received attention. Most of these attentions were based on the research effort conducted in the industry and in the field of academia [61]. VANET is classified as a key technology in intelligent transportation systems. VANET is envisaged as playing an important role in the futuristic smart cities. This important role in VANET improves road safety and also provide innovative services relating to traffic management and information achievement applications. Thus, it has become expedient for creating a wide range of services for future VANET deployment that ranges from safety/security and traffic management to commercial applications services [62]. Offering



these services requires high QoS guarantees. Without QoS guarantees, these services would not be successfully achieved. Due to the highly dynamic nature of VANET, resources reservation for services are not applicable for providing a QoS guarantee.

In addition, two communicating vehicles that are moving would experience a degrading performance. This can be possible when the wireless links formed between them are vulnerable and the vehicles are disconnected due to DoS attacks. This can lead to unpredictable driver performance. QoS metrics such as throughput and jitter associated with the current routes established changes rapidly. The best selected routes computed by the RSU could easily become inefficient and lead to infeasible routes due to imminent links breakdown. Thus, utilizing a search for feasible route in multihop VANET is subject to multiple QoS constraints.

### 5.2.1 QoS Results and Analysis for the Proposed Scheme

The result and analysis of the proposed SIVNFC scheme is compared with the other contending models such as: CSA (Cuckoo), FA (firefly), and the firefly neural network. The analysis is based upon the QoS provision determination in VANET. The QoS analysis is based upon the simulation result and the mathematical analysis of the models in the SAPM. The QoS investigation is centered on throughput and jitter associated with the current routes that has been established in the network as a result of rapid changes in the network due to the result of DoS and SNI in the VANET. We determine the QoS as follows:

- Throughput: It is the total number of delivered packets in the given time frame.

$$\text{Throughput} = \frac{\text{Total}_{\text{delivered}}}{\text{Time}_{\text{frame}}} \quad (16)$$

Latency/jitter: It is the total delay that is produced when delivering data packets in the network.

The evaluation of the parameters is obtained in such a manner that the Packet Injection Rate (PIR) is on the x-axis and the QoS evaluation parameter is on the y-axis. The PIR is the ratio of the injection of the packets into the network. Figure 5.2 demonstrates the results of the proposed SVINFC scheme, which is compared with all the other contending models. The proposed SIVNFC scheme considers the throughput with Cuckoo, firefly, and the firefly neural network. The range of PIR is from 0.001 to 0.02. With the increase in the PIR, the throughput increases, which is also demonstrated in Figure 5.2. The maximum throughput at PIR = 0.02 is 8100 for the proposed SIVNFC scheme and 7900 for the firefly–neural network model. One hundred packets are injected per millisecond.

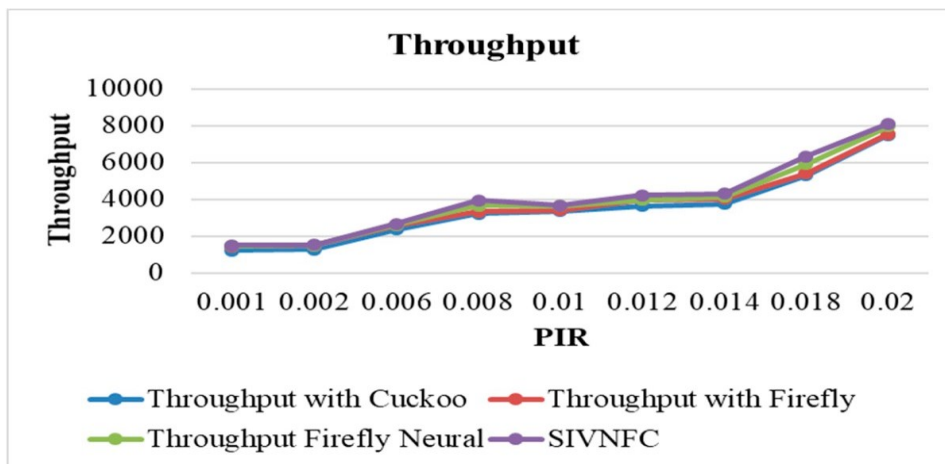


Figure 5.2 Throughput Versus PIR.

<b>APPROACHES</b>	0.001 PIR	0.002 PIR	0.006 PIR		0.008 PIR	0.01 PIR	0.012 PIR	0.014 PIR	0.018 PIR	0.02 PIR
CUCKOO	1100	1150	2300		3100	3300	3600	3800	5200	7500
FIREFLY	1200	1255	2350		3200	3400	4000	4000	5300	7550
FIREFLY NEURAL	1250	1300	2500		3700	3600	4050	4100	6000	8000
PROPOSED	1500	1550	2750		4000	3650	4150	4250	6200	8100

Table 5.2: Throughput of the Proposed Scheme Compared to the other Contending Model at Various PIR

The second evaluation parameter is the jitter. Jitter produces delays when the network experiences DoS and SNI. However, due to the fact that the proposed SVINFC scheme has introduced fog computing and that trust between the communicating neighboring nodes has been established, the entire network level security is increased. This has also led to decreased communication costs and time. The route that is discovered and assigned as trusted is stored on the fog server. Due to this, the need for broadcasting is reduced for route discovery and much time is saved. The evaluation of the jitter is done considering the same aspects as the throughput.

The jitter is not a consistent parameter in any network. Figure 5.1 shows that the

jitter may be high or low for different PIR values. Throughout the PIR, the proposed SIVNFC scheme is noted to produce the least jitter when compared to other contending models' scenarios. Though the fog computing server is applied to all the scenarios, the max jitter for the SIVNFC scheme is 96 ms, whereas the maximum jitter for Firefly Neural is 102 ms. Figure 5.2.1 shows the effect of varying the throughput of the proposed scheme and the other contending schemes including the Cuckoo, Firefly and the Firefly neural. It is based upon the packet injection rate (PIR) in the network system.

The throughput in every network system is generally expected to be high, as it is examined through various PIR, in order for the network devices to communicate efficiently. Based upon the graph depicted in the figure 5 the throughput graph of the proposed scheme shows significant high, compared to the other contending models as depicted in table 2 at various PIR.

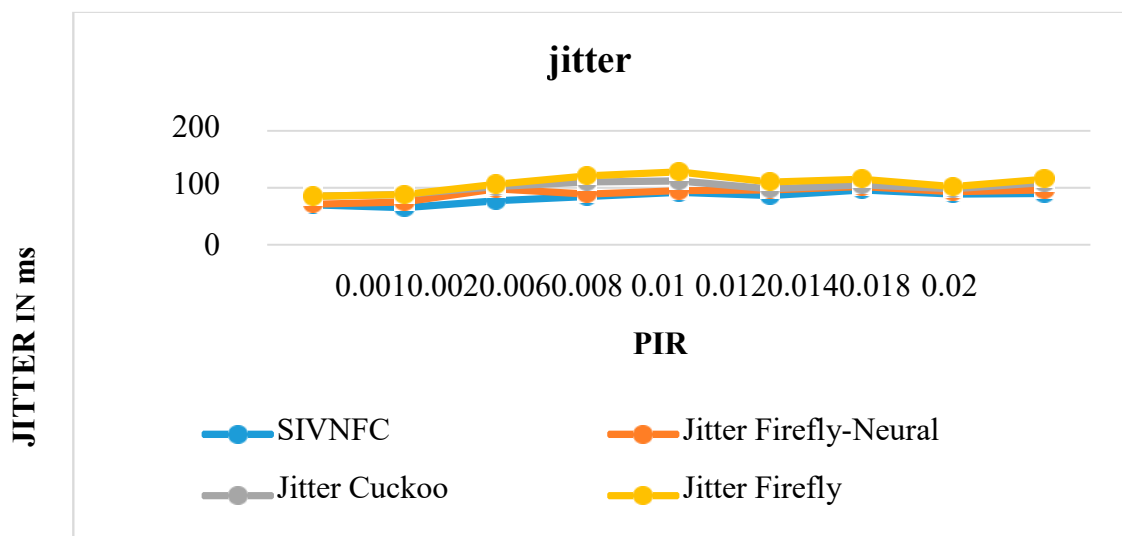


Figure 5.2.1 Jitter Versus PIR

	<b>JITTER</b>								
<b>APPROACHES</b>	0.001 PIR	0.002 PIR	0.006 PIR	0.008 PIR	0.01 PIR	0.012 PIR	0.014 PIR	0.018 PIR	0.02 PIR
CUCKOO	83	88	102	110	114	99	106	99	110
FIREFLY	84	89	104	120	128	114	118	102	119
FIREFLY NEURAL	72	78	98	88	97	98	103	96	98
PROPOSED	70	64	78	82	92	85	97	89	90

Table 5.2.1: Jitter of the proposed Scheme Compared to the other contending model at Various PIR

Figure 5.2.1 shows the effect of jitter introduced in the network system based upon varying number of known and unknown distributed DoS and SNI attacks in the network. The jitter is evaluated based upon various PIR of the network system received by the proposed scheme SIVNFC, compared to the other contending models such as Cuckoo, Firefly and Firefly neural. The jitter in every network system is expected to low, in order for the network devices and the entire network system to deliver efficient packet and also communicate efficiently. As shown also in Table 5.2.1 the proposed scheme jitter shows significantly less at various PIR.

# **CHAPTER 6: REAL-TIME DETECTION OF DoS ATTACKS IN IEEE 802.11P USING FOG COMPUTING FOR SECURE INTELLIGENT VEHICULAR NETWORK.**

## **6.1 Introduction**

VANET is a popular network of this modern frame. The network is termed as an ad-hoc network, as the position of the vehicles changes at every instant of time. The average speed of vehicular nodes varies from 40-80 km/h [63]. 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 subclass of MANET (Mobile ad-hoc network) for providing communication along with nearby vehicles and among vehicles close to roadside unit (RSU) or equipment, though diverse from other network according to their characteristics [64]. Particularly, the vehicles (nodes) are inadequate to road topology when moving; thus, vehicles' future position can be predicted when information of the road is available.

As per IEEE 1471-2000 and ISO/IEC 42010 framework general guidelines, VANET system can be categorized into three domains including: Mobile, infrastructure and generic domain [65].

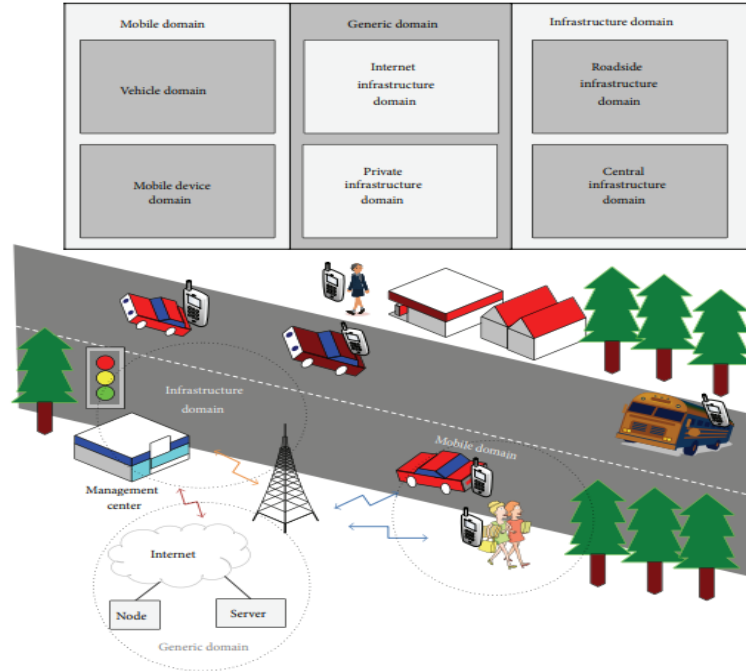


Figure 6: VANET Infrastructure Architecture (VIA)

Mobile domain is composed of two parts (please refer to figure 6.1 for detail description). Infrastructure domain consists of two parts (please refer to figure 6.1 for detail description); 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/indirectly for VANET.

Figure 6 depicts the VANET infrastructure architecture (VIA). The mobile domain transfers the information and communicates with the infrastructure domain. It utilizes IEEE 802.11p beacons/signal that processes the data and proceeds towards for modulation [66]. Then, the infrastructure domain communicates with generic domains and then exchanges the information. The flows of data between the mobile and stationary resources result in effective utilization of road with the user which utilizes IEEE 802.11p beacon

communication standard.

In this research, the transmission rate of information for real-time IEEE 802.11p information delivery in VANET is 30Mbps. Vehicles move in group, as they are directed in the VIA to their intended destination (as shown in Figure 6). In the VIA also, vehicles cooperation in the group movement are such that they exchange frequent sporadic broadcast of safety message. This carry the information of the speed of the vehicle and their position whilst utilize the IEEE 802.11p beacons dedicated channel [67]. During normal operation of the IEEE 802.11p medium access control (MAC) protocol random access specification, beacons lost is possible. This can be attributed to impairment of wireless channel (i.e. beacons transmission overlapping, resulting from several vehicles, which can lead to collision/congestion).

Collision/Congestion (CC) can be reduced based upon proper selection of MAC protocols real-time transmission methods which include secure authentication/ key distribution algorithm models, and secure transmission range models, that can be deployed in the VIA network. Based upon this performance parameters, such as real-time end2end delay sensitivity for trust enforcement of neighboring nodes in VANET can be measured [68] [69]. Nevertheless, it is possible that the IEEE 802.11p beacons transmissions can also get corrupted through malicious attacker vehicle. This may also present themselves in all forms of attacks including hybrid DoS attacks (HDSA) which include: DoS jamming signal attack DoS (JSA), packet drop (PD) and resources consumption/RSU or CPU overutilization (RCRCO) [70].

The VANET safety can seriously be at risk, since vehicles would not be capable



to properly utilize the information obtained. However, vehicles are required to utilize and transmit the information based upon the IEEE 802.11p beacons relay through the RSU, in order to sensitize awareness in VANET. The RSU utilizes the information to also updates other vehicles about the requirement of end2end delay/jitter in the network, which has been imposed by the automotive control system (ACS) from traffic management center as shown in the VIA in Figure 6.

Consequently, real-time detection of all forms attacks, including hybrid DoS attacks (HDSA) require trustworthiness, intelligence 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 integrate with authentication/KDE mechanisms. This integration with the other real-time detection of HDSA can provide secure methods in the MAC layer. This can be used for mitigating all forms attacks including HDSA such as: DoS JSA, PD and RCRCO, which utilizes IEEE 802.11p beacons transmission in VANET. This represents an urgent practical problem in which we are motivated in this research for investigation.

### **6.1.1 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 the studies in [71] [72]. In these studies, MAC layer misbehavior of some vehicle/nodes violates IEEE 802.11 rules. They chose small back-off counter to access the channel frequently than other nodes. However, their performance was

degraded. These investigations were studied, however, restriction in detection of all forms of attacks, including HDSA was an issue. Moreover, the investigation was based on only DoS JSA attack. In detecting DoS JSA only in VANET, the method in [73] utilized unicast traffic method based upon 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 IEEE 802.11p vehicular network method was also proposed in [74].

This is 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 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 all other forms of attacks eminent in VANET, which include HDSA in VANET. The detection of all other attacks and HDSA still presents 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 [75,], which mostly cause overutilization of the RSU. However, none of the above defined proposed schemes in VANET considered investigation for detecting HDSA, which also include DRA. Moreover, the authors investigation concerning utilizing the above proposed schemes demonstrate only limited recommendation and provision for: trusting

methods, secure efficient storage mechanism and proper OAs and authentication/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 attack encompass DRA for the sake of this research. Therefore, it is important to investigate HDSA using sophisticated approach. This new approach will be capable to detect all forms of DoS attacks, including the HDSA attacks, which should be supported in this research.

VFC (vehicular Cloud and Fog Computing) is a standards that comprehend FC and vehicular cloud (VCC) [76]. VFC is also a solution that satisfies the requirement of VANETs such as secure and efficient computing, storage and in-networking resources provision [75]. In addition, optimization algorithms (OAs) such as: Cuckoo/CSA (ABC) [77], Firefly algorithm (GA) [78] and firefly neural [79] are capable to provide swarm intelligence. The OA are either heuristic or metaheuristic in nature that have problem solving skills. They also have the capability to adjust DoS JSA and HDSA (i.e. congestion/collusion), which include all other forms of attacks: DoS JSA, PD and RCRCO, for optimum user experience [80].

The OAs have also been used to evaluate a real-time data transmission in VANET[81], which utilized the 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 methods for VANET protection provide a real-time detection of DoS attacks in IEEE 802.11p which utilizes the DSRC technology. It also provides safety of roads and highways based upon intelligent transportation systems (ITS)

opportunities. Therefore, real-time detection of DoS JSA and HDSA utilizing IEEE 802.11p, which is based upon VFC require investigation for evaluating end2end delay/jitter in VANET, due to DoS JSA and HDSA attack (congestion/collision) for trust evaluation.

The authors in [76], [77], and [78] have conducted investigation separately in Cuckoo/CSA (ABC) and Firefly Genetic Algorithm (GA) respectively. The investigation was used for evaluating delay sensitivity for real-time detection for only DoS JSA attack in VANET, which also utilized DSRC technology. However, based upon the investigation conducted with Cuckoo/CSA (ABC) scheme, it revealed that it was not centered on VFC. In addition, most of the scheme's investigation dwell on only unicast method for data transmission. However, this did not achieve trustworthiness in the network. The authors have conducted 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 path 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 that include: DoS JSA, PD, and RCRCO in the network. In addition, absence of VFC method was also major limitation observed in the schemes. Therefore, it can be concluded that there is trustworthiness limitation in VANET. This still presents greatest challenges.

To address these challenges in VANET, in this research, we consider all forms of attacks including all forms of DoS attacks detection in VANET which also include but not limited to: DoS JSA, HDSA (congestion/collusion), PD and RCRCO/DoS attack, in our

proposed scheme VIA models. We also consider the hybrid deployment of OAs with VFC and integrates full authentication/KDE trust mechanism deployment in the VANET. These will be used for evaluating the end2end delay/jitter in real-time IEEE 802.11p hybrid multicast and unicast data transmission in VANET. Therefore, in this dissertation we propose real-time detection of DoS attacks in IEEE 802.11p using VFC in Secure Intelligent Vehicular Network.

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 advantage 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 attacks detection such as: DoS JSA, PD and RCRCO in VANET, to provide trustworthiness in the network.
- Provision of IEEE 802.11p benefit of information processing which utilize hybrid multicast and unicast broadcast data transmission in VANET for efficient and real-time transmission of safety information exchange.
- Provision for single next hop vehicle (SNHV) probability analysis for efficient data processing, within elliptical segment area transmission range (ESATR) in VANET.
- Provision for regression model prediction based upon reduced delay/jitter in VANET

for secure road safety provision in VANET.

The rest of the chapter is organized as follows. Section 6.2 presents the related work. Section 6.3 presents the secure real-time detection of DoS attack model (DAM) and Jamming signal attack model (JAM). Both attack models provide Hybrid DoS attack model (HDAM) prevention mechanism in VANET. Section 6.4 presents the preventive mechanisms and the System models including: System architecture model (SAM) and Elliptical segment area transmission range model (ESATRM), OAs deployment and trustworthiness of nodes of the proposed scheme. Section 6.5 presents the result analysis discussion. Section 6.6 is the Background study comparison of VANET protocols and Section 6.7 presents the conclusion.

## **6.2 Secure Real-time Detection of DoS Attacks, Prevention Measures in VANET**

### **6.2.1 Hybrid DoS Attacks (HDSA)**

Hybrid DoS attack (HDSA) employ HDSA models. These models are designated as the proposed scheme attack models. It also encompasses all the attack models that mitigate: DoS JSA, PD, and RCRCO (RCRCO/DoS attack) 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 including all DoS attacks and 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, anticipated in the proposed scheme of this research.

### **6.3 DoS Attack and Model**

Denial-of-service (DoS) attacks has target to block availability of computing systems and networks services, and therefore it requires DoS attack model that can be used to mitigate these attacks. DoS attacks also overwhelms 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 accurately as required and effectively. The computing system also deny services to legitimate users [82]. In addition, as a substitute for the system to function appropriately, it would rather perform other irrelevant functions not required in the network.

All forms of DoS attacks including HDSA model such as: DoS JSA, PD, and RCRCO (DoS attack model), can be experienced through insiders and outsider malicious intruders of the network. This halts providing network availability to its real users. It occurs through flooding of the control channel with naturally generated illegal and malicious message sent at a high speed [83]. A DoS attack/ RCRCO key resources include high bandwidth demands, CPU/RSU overutilization and excessive memory computations. DoS attacks/RCRCO have the tendency to reduce the speed and volume of legitimate network by consuming high bandwidth resources. Through DoS attacks/RCRCO, packet processing and network device could be prevented and not respond to management request. This might

effectively lock the devices by consuming excessive memory leading to CPU/RSU overutilization of resources.

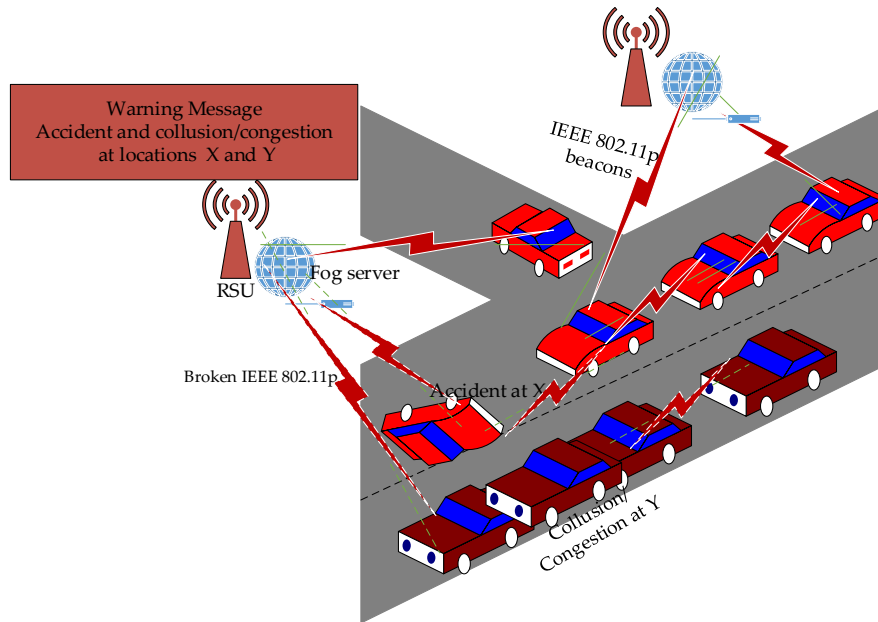


Figure 6.3: Hybrid DoS Attacks Model (DAM)

Figure 6.3 depicts 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 HDSA occur, it results to accidents at locations X and Y. Another scenario of DoS attack/RCRCO include high bandwidth, CPU/RSU overutilization and high memory computation, which also leads to broken signal. Since vehicles cannot appropriately utilize the 802.11p beacons for message transmission, it will lead to collision/congestion of other vehicles. Consequently, this will also lead to encounter of broken IEEE 802.11p beacons signal. This act also leads to not being able to acquire fully the IEEE 802.11p beacons/signal, which results in end2end delays of the network.



Moreover, packet drop (PD), false information (FI) and jamming signal attack (JSA) encounter in VANET is possible. In the other scenario, normal vehicles which are travelling to their intended destinations communicates with each other vehicles. The vehicles utilize the unbroken 802.11p beacons/signal that encompass: V2V, V2RSU and RSU2RSU. Based upon this scenario, the RSU and fog server connection can be achieved through either by wired means or by wireless means. The connections of the RSU and FS utilizes the unbroken 802.11p beacons/signal with the road-side unit to vehicle (RSU2V) communication, and vehicle to roadside unit (V2RSU) communication to process information in the network.

The RSU2V, V2RSU and V2V effective signals communication of the unbroken IEEE 802.11p beacons signals can also be achieved through the fog server (FS) connection with the RSU. These connections which are secure, utilize the IEEE 802.11p beacons/signals, generated from the accident scenarios to sensitize awareness of the road conditions. The scenario may also represent congested/collision of vehicle that is used as a standard for safe information dissemination to other vehicles and road users. Based upon this, all other normal vehicles which have not yet encountered congestion/collision and accidents, will appropriately be informed about any accident and collision/congestion situation, which have occurred, such as at locations X and Y. Moreover, the broken IEEE 802.11p beacons signals are intended to cause end2end delay in the VANET which will require evaluation in network performance metrics.

When accident occur, it would prevent timely relay of the IEEE 802.11p beacons, leading to PD, FI and DoS JSA. Therefore, through this research, we launch further

investigation for evaluating the presence of all forms of attacks including HDSA, PD/FI and DoS JSA, using attacked packet detection algorithms. The anticipation of proposed system architecture model (PSAM) implementation, for detecting packet drop PD/ FI, for DoS JSA scenarios are also important component of this research, whereby HDSA model requirement should be investigated for VANET. Now, we try to understand PD/FI and DoS JSA which include HDSA detection.

### **6.3.1 Packet Drop (PD) and False Information (FI)**

Packet drop (PD) DoS attack (PDA) including FI, is one of the attacks that originates from HDSA model. It may occur due to interference of 802.11p beacons that may be present in the PSAM of the proposed scheme. PDA may also lead to end2end delay of path detection of the communication process in VANET, during the deployment of V2V, V2RSU and RSU2V communications in the network. On the other hand, PDA will also lead to FI message delivery in VANET. FI may also represents wrong or fake information generated through packet drop (PD), which has resulted from all forms of attacks including DoS attacks. Thus, PDA might be sent purposefully by a node to other node in the network that has the tendency to create congestion/collision (CC) traffic scenario. 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 DoS JSA since the road becomes available for attackers to exploit them for their own purpose. Therefore, it is important that DoS JSA should be considered for investigations in

the PSAM.

### **6.3.2 DoS Jamming Signal Attack (DoS JSA)**

DoS jamming signal attack (DoS JSA) represents a high form of DoS attacks that have been investigated mostly by researchers. It is also a component of the HDSA model proposed in this research. During DoS JSA encounter, the attacker usually jams the channel, which can be represented as the congestion/collision scenario in VANET. DoS JSA has a main objective for a jammer to trick a legitimate IEEE 802.11p beacons signal communication and reduce or degrade the overall VANET performance. During DoS JSA encounter, network users are not permitted to access the network. This may usually cause the broken IEEE 802.11p beacons signal and introduce end2end 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 packet is 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 beacons radio signals continue to be emitted. With reactive RDJA encounter in VANET, resources are wasted, and the receiver is targeted when more noise encounter in the data packet occur. RADJA effects can be experienced in two modes. In the first mode RADJA leads to excessive traffic encounter of traffic for random intermittent of time. Whereas in the second mode, RADJA leads to stopping of transmission of the signal for another random intermittent time frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSP) [84].

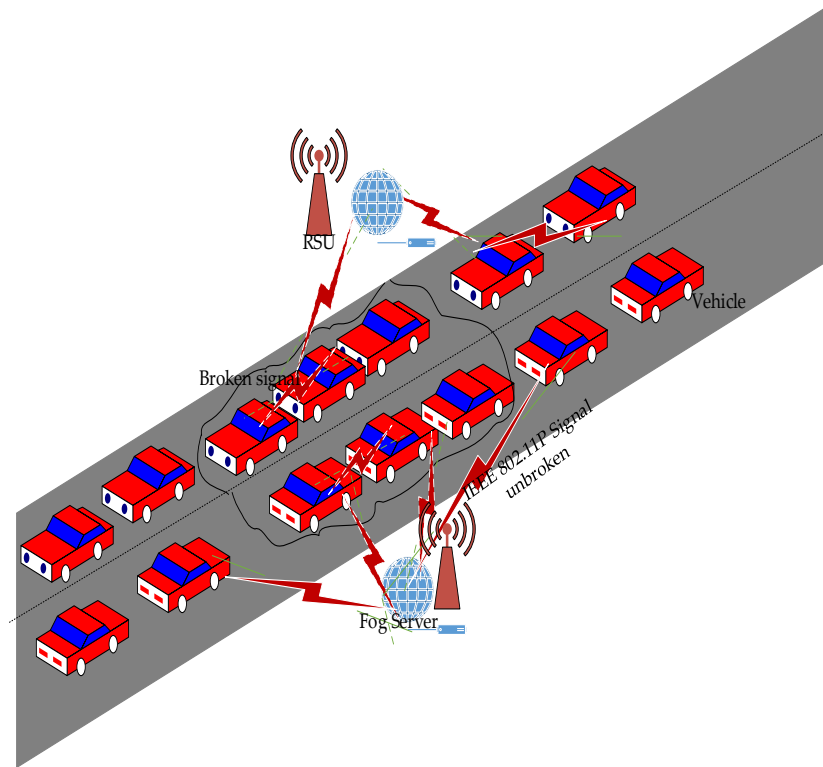


Figure 6.3.2: Vehicular Communication DoS Jamming Signal Attack Model (D JSAM)

Figure 6.3.2 represents vehicular communication DoS jamming signal attack model (DJSAM) scenario of the proposed scheme that also serves as component of the HDSA model (HDAM). In the figure there are two scenarios. In the first scenario are normal vehicles which utilizes the IEEE 802.11p unbroken signals. The unbroken signals are also utilized to initiate V2V communication to sensitize each vehicle about safety information of the roads, and DoS JSA situation that have occurred. This can be achieved through the connection of the RSU which is either wired or wirelessly 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 which are moving within a specified communication range, encounter actual channel DoS JSA situation. The second scenario also include utilizing the IEEE 802.11p broken signals. The broken signal communication scenario incurs unacceptable end2end delay in the network through: V2V and V2RSU and RSU2V that would also convey 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 end2end delay on the path of each vehicle in the network would be needed. This requires using sophisticated system architecture model of the proposed scheme such as PSAM (will be explained shortly).

The PSAM is required to utilize attacked packet detection algorithms combined with HDAM model, which will be beneficial to detect the end2end delayed path of all HDAM attacks which include: DoS JSA, PD, RCRCO and all form of associated attacks in the network that has capability to introduce end2end delay/jitter. This is implemented in the prevention mechanism and the PSAM of the proposed scheme.

## **6.4 Prevention mechanisms of the proposed scheme**

### **6.4.1 Proposed Scheme System Architecture Model (PSAM)**

. In this research, PSAM represent the proposed scheme system architecture model. It is used for the detection of end2end delayed path packet of vehicles in the network. PSAM utilizes the attacked packet detection algorithms (APDA) deployed in the PSAM as shown in Figure 6.4.1. The APDA is utilized to capture all forms of attacks categories including HDSA and all other forms of associated with VANET, as identified

with the PSAM. The HDSA category include PD/FI, DoS JSA, and RCRCO that would require high memory computation and high bandwidth. Below in Figure 6.4.1 depicts the PSAM of this research, whereby the APDA have been implemented. The APDA method used are attached through every RSU and the FS via a packet detection mechanism that distinguishes exact messages position on the path of vehicles that utilize ESA communication range (ESACR), which has the objective of evaluating end2end delay/jitter experienced in the network.

In addition, RSU main job functions include serving as a gateway for the PSAM for all vehicle's communication. The RSU also coordinates with FS to disseminate secure transmissions of V2V communication. The RSU is also connected with the FS through wireless or wired means. After the detection of vehicle position, the information or messages are derived based upon the effectiveness utilization of the above two attacks models which include: DoS JSA models (DAM) and jamming attack model (DJSAM). These two models (DAM and DJSAM) are together known as hybrid DoS (HDAM), which is deployed for the proposed scheme for detection of the HDSA and other attacks, discussed previously in section 3. HDAM as depicted in Figures 6.3 and 6.3.2, utilize RSUs and the FS to process the communication.

Thus, HDAM utilize the IEEE 802.11p beacons/signal. IEEE 802.11p beacons employ the devices in the VANET, which have OBU (Onboard unit) and TPD (Tamper Proof Device), for storing the comprehensive information for the vehicles like: position, speed etc. The position of vehicles is identified by the velocity of vehicles, frequency of the vehicles, the vehicle position and the number of packets sent to the vehicles. The

vehicle position identifications utilize the following communication process: vehicle-to-vehicle (V2V) communication, vehicle-to-road-side unit (V2RSU) and inter-roadside – communication unit (RSU2RSU), as shown in Figure 6.4.1. The communication process also encompasses the relay of IEEE 802.11p beacons through hybrid multicast/broadcast and unicast data transmission. The communication process also sensitizes awareness for the road safety and driver’s vigilance.

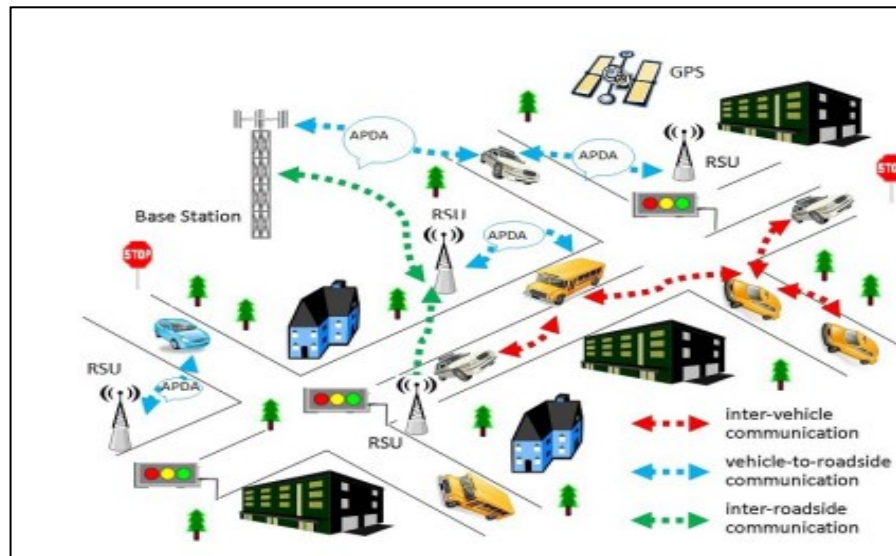


Figure 6.4.1 Proposed system architecture model (PSAM) for proposed scheme

In the PSAM, when the packet is not attacked, then the V2V communication, V2RSU, RSU2V and RSU2RSU would not track the path in end2end delayed 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 requirement as per the variations in the positions of vehicles in the VANET. The identification of the attacked packets can be done by V (velocity), F (Frequency),  $\lambda$  is a co-efficient that has been

determined by the characteristics of road and  $V_{max}$  is the maximum Speed as shown in the Equation (1):

$$F = \lambda * \left| V - \frac{v_{max}}{2} \right| \quad (1)$$

F is the number of packets unicasted and multicast (or broadcasted) per second. The identification of the attacked packets is done by the below conditions:

The range of F and V is high as the position would vary instantly.

The range of F and V is low as the position of vehicles would not vary instantly.

The algorithm is based upon the variation in frequency, position, and velocity. The algorithm for the detection of attacked packets is defined below:

---

**Algorithm 6.4.1:** Detection of all attacked packet based on HDSA and other attacked packets

---

1.     **Function** RECOGNIZE (attacked packet for HDSA in the models).
2.     Start
3.     Discover  $F = \lambda * \left| V - \frac{v_{max}}{2} \right|$
4.     **If** (F>=high&&V>=high) **then**
5.         recognize (Attacked packet)
6.         set attacked packet detection Alg (req) **then**
7.             Start when validated (request)
8.     return true
9.     **else**
10.     **if** (F<=low && V<=low) **then**



11. return invalid request
  12. **else**
  13. set attacked packet detection Alg (req)
  14. **end if**
  15. **end if**
  16. **end**
  17. **end**
- 

The above algorithm can be applied prior to the verification time and for increasing the security. The algorithm is utilized for detection of unacceptable requests with the attacked packet. It can also be utilized to avoid the end2end delay CO, on the path of vehicles in the network. It is also worthy to note that establishment of a safe and secure root is another thing and sending the data in secure manner is also another thing. Even if the roots are safe, it cannot be 100% trusted. The proposed scheme models utilize Vehicular RSA algorithm (VRA) type at the transmitter end. The transmitting node also shares a key to the universal port (A ports which keeps an eye of 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 intermediary who can verify it. The central port plays the role of the intermediary. The receiving node and the transmitting node both send their key added with 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 have 6612 and assume that the registration number of the receiver is 45 then the key which is shared by the receiver is  $6612+45=6657$ . The central

port subtracts the registration number from both the sender and transmitter shared value. If after the subtraction, both shared 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 is shown below.

---

**Algorithm 6.4.2:** Vehicular RSA Encryption algorithm

---

1. **If** Sender vehicle  $S_v$  creates a key **then**
2. 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
3. Set  $S_v$  and  $R_v$  to determine the value of large number N using,  $N = PQ$  **then**
4.  $R_v$  and  $S_v$  Creates the value M //using the given expression below, based upon Euclidean algorithm
5.  $M = \phi(N) = (P - 1)(Q - 1)$
6. **If**  $S_v$  and  $R_v$  select any integer value E **then**
7.  $E =$  positive integer // E lies between,  $0 < E < M$
8. Function  $\text{GCD}(M, E) = 1$  // (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
8. **If**  $(E * D) = 1 \pmod{M}$  **then**  
 $(E * D) \pmod{M} = 1$  &
9. **If**  $S_v$  and  $R_v$  create the Public key: E, N **then**
10. Set  $S_v$  and  $R_v$  to create Private Key using D and N
10. Encryption / Verification:

11. **If**  $S_v$  and  $R_v$  can utilize original plain text (a block value) =  $X \dots X < N$  **then**
  12.  $S_v$  and  $R_v$  Obtain Ciphertext =  $C \dots C = (X^E) \bmod N$
  - End if**
  13. Decryption / Signing:
  14. **If**  $S_v$  and  $R_v$  Utilize Ciphertext =  $C$  **then**
  15.  $S_v$  and  $R_v$  utilizes Deciphertext =  $Y$
  16. **End if**
  17. **End if**
  18. **End if**
  19. **End if**
  20. **End**
- 

Proposed Vehicular RSA is an algorithm used by modern fog computing and cloud based technique 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 key can be given to everyone. The other key must be kept private.

Figure 6.4.2 represents the authentication process of data packets using vehicular special type of RSA encryption algorithm. The transmission of data packet from transmitting vehicle/node to the receiving vehicle/node is represented by an arrow. Every vehicle in VANET comprises of an individual private key generated by each node along with the public key. Public key is same for every node whereas private key is different. Therefore, whenever a node wants to transmit the data, a private key along with public key has been generated and transmitted along with the packet. In case when the key is matched it means that the node is genuine, and the transmitting node transmits the data else consider

the node as an attacker node and change the route without forwarding data to the attacker node.

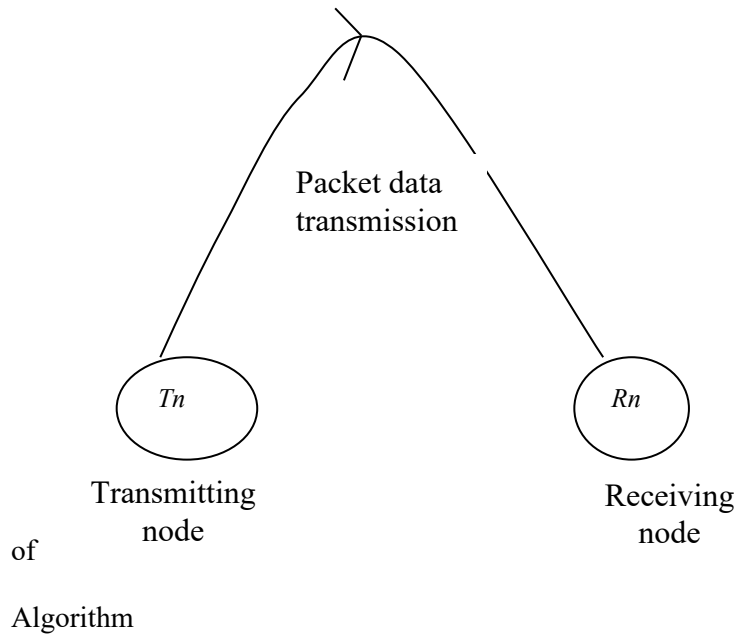


Figure 6.4.2: Authentication Data Packets using Vehicular RSA Encryption

The process of authentication of data packet in the proposed scheme models is also required to be extended for further investigation on storage of data in a model, based upon the ESA which was determined based upon the DJSAM elliptical segment transmission range. This is due to the fact that there is high anticipation of DoS JSA that is 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 that utilizes ESA, is important in the network design for solving limitation in storage and computation of VANET. VFC should also be deployed in elliptical segment area transmission range (ESATR), in order to also investigate for trust, using storage prevention mechanism in the proposed scheme network, which will be investigated subsequently.

## 6.5 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 which denotes VFC can store a lot of data which can be reused and can be aggregated to prevent time successions search, as the vehicles do have much onboard storage [85]. 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 to know that packets are either received effectively or not. When the vehicles in the cloud have the data packets, then vehicles verify to know 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 state election mode. Later, vehicles unicast the received packets towards the parent cloud to send the packet till packets arrive at the cloud leader which discloses about the vehicle information. Accordingly, as shown in the below algorithms, if the cloud leader produces a data packet, initially it verifies about the packet source.

When the data packet approaches from encode-B (an element of LTE (long term evolution) 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 LTE data packet ( $LTE_{dp}$ ); which transfer the packets to the enode-B with the novel original received packet from the vehicle. In the end, the packets are updated as CLvInf (Cloud leader vehicle information). The PSAM utilizes the multicast/broadcast and unicast modelling in order to fulfill the requirement as per need. Obviously, the multicast architecture incurs some latency and as it broadcast the data, it will consume some time.

---

**Algorithm 6.4.3:** IEEE 802.11p-LTE CM

---

1. On  $d_p$  generating or receiving: // on receiving or generating the data packet
  2. filter  $Id_{data}$  or  $req_{data}$ ; // Filter on Packets
  3. **If** ( $Id_{data}, req_{data}$ )  $\in$  CLvInf &
  4. **If**  $d_p$  is from  $pr_c$  **then**
  5. multicast On  $d_p$  to CM; // Multicast situation
  6. **else**
  7. unicast  $d_p$  to  $pr_c$  CL // Unicast situation
  8. Update vInf;
  9. **end if**
  10. **end if**
  11. **end**
- 

---

**Algorithm 6.4.4:** IEEE 802.11p-LTE CL

---

1. **for** On  $d_p$  generating or receiving **then**
2. filter  $Id_{data}$  &  $req_{data}$ ;
3. **If** ( $Id_{data}$  ,  $req_{data}$ )  $\in$  CLvInf &
4. **If** (On  $d_p$  is from eNodeB) **then**

5. Send On  $d_p$  to CM;
  6. **Else**
  7.     broadcast  $d_p$  to CM
  8.     develop  $LTE_{dp}$  and send to eNodeB **then**
  9.         Update vInf;
  10.     **end if**
  11. **end if**
  12. **end for**
  13. **end**
- 

**Algorithm 6.4.5:** IEEE 802.11p-LTE eNodeB

---

1.     **For**  $d_p$  generating or receiving.
  2.         filter  $Id_{data}$  and req\_data
  3.     **if**  $(Id_{data}, req_{data}) \in (CL, vInf)$  **then**
  4.         broadcast  $LTE_{dp}$  to eNodeB-fog **then**
  5.             broadcast  $LTE_{dp}$  to CL **then**
  6.                 send to server-fog **then**
  7.                     broadcast  $LTE_{dp}$  to eNodeB **then**
  8.                         broadcast  $LTE_{dp}$  to CL
  9.             Update eNodeB;
  10.         **end for**
  11. **end if**
  12. **end**
- 

Algorithms 6.4.3, 6.4.4 and 6.4.5 defined above decrease the issues of the broadcasting storm within the network, by lessening the iterated data broadcasting and by

keeping less overhead information. It also broadcasts the specific data by appropriate vehicles or the nodes that also decreases the network load. The reduction of network load action taken is necessary, due to consideration of overwhelming messages that may occur, as result of all forms of attacks and HDSA in the network. It also lessens the problem of network disconnection by lessening the regular downloading and subscribing to the network [86]. Table 1 depicts the notation and descriptions of the algorithms and the model's terms.

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

## **6.6 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 utilizes HDAM, is designated in the network. The designated transmission range is based upon 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, involvement in HDAM is also important for investigation. It requires further authentication prevention mechanism in the network. Therefore, this research investigates about a model in VANET known as the proposed scheme elliptical segment transmission range model (PESATRM).



PESATRM include the tendency to utilize secure authentication prevention method which is integrated in VANET communication process design for also mitigating HDSA. Secure authentication in the PESATRM can be achieved through FS and the RSU deployment. In the PESATRM, V2V vehicle communication process utilizes IEEE 802.11p beacons transmission to communicate and also secure the network links. This provide the capability for each vehicle to exchange messages securely, within a specified ESATR. Based upon this, vehicles move along in the same direction of travelling to their intended destination (as shown in Figure 6). Therefore, the PESATRM has been developed from modified circular segment area model (CSAM) adopted in [87].

However, investigation reveal that the CSAM is insecure based upon limitation in HDSA, and all other forms of attacks investigation. In addition, another limitation worthy to know is that the CSAM design did not utilize fog computing and cloud-based (VFC) integration investigation. Therefore, it is anticipated that the PESATRM communication process should be designed to include VFC that employ authentication/KDE (AKDE) to further secure the network. In addition, it is estimated that designing a secure PESATRM would also prevent high incidence of communication overhead (CO). CSAM limitation also include increased communication overhead (CO).

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 end2end delayed path packet detection process. This is based upon the fact that NV2NV (neighbor-vehicle-to-neighbor-vehicle) communication process requires further AKDE. Moreover, SRSIE process that prevents CO, due to end2end 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 DoS attacks including HDSA, which utilizes IEEE 802. 11p beacons transmission relay process in a specified ESATR.

Furthermore, in the design of the PESATRM, rapid topology changes in VANET is important for investigation. This is because, HDSA including DoS JSA and other vulnerabilities are eminent in the air, or in the open environment in which VANET deployment. Therefore, the PESATRM is also designed to detect traffic in DoS JSA and its associated vulnerabilities faster and accurate. The network topology design should utilize VFC and AKDE, which is able to store large volume of data utilized for secure delivery of SRSIE. Based upon this provision, it possible for the proposed scheme to detect and mitigate HDSA and associated vulnerabilities that would incur CO in the network. In addition, VFC provide 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 utilize 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 utilize HOA heuristics for solving problems in the network such as end2end delay/jitter performance evaluation. Based upon this, dynamic transmission range is provided in the network. Dynamic transmission is usually more effective in maintaining connectivity. HDSA and all other forms of Dos JSA can be detected and eliminated from the network when specified ESATR is deployed in the PSAM

and the PESATRM integration. We also anticipate that the design of ESATR should be more secure.

Comparatively, the circle segment transmission range (CSAM) in which PESATRM was modified from is more confined. Therefore, we anticipate that the CSAM 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 7.5 is used to explain the deployment of the PESATRM. It is anticipated logically for the PESATRM utilize AKDE. In Figure 6.6 (as shown below) the vehicles within the ESATR are also known as neighbors. These neighbor vehicles (NV) are secure in the network using AKDE method. NV are also required to keep one global key (Gk). The Gk provides requirement in authentication of the NV 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 every NV using NV2NV communication. In addition, secure sharing of the Gk include SRSIE accurately. Therefore, implementing 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, NV exchange hello messages to initiate the communication process. Thus, NV are capable to utilize sufficient time in the NV2NV communication to be able to transmit SRSIE. This successfully led to processing of standardized road safety traffic emergency information (SRSIE) exchange for VANET in the same ESATR.

Based upon this, Figure 6.6 also depicts the PESATRM, which utilizes V2Vcommunication. The PESATRM NV exchange hello neighbor messages. The hello message exchanged by NV is initially broadcasted/multicast and finally unicast using NV2NV and secure NV communication. NV2NV and secure NV communication process include neighbor vehicles (NV), origin vehicles (OV), and the destination vehicle (DV). Each NV that forms communication with each other NV initially gets authenticated. Afterwards, NV transfer the Gk securely with each other. Subsequently, NV or NV2NV simultaneously transmit SRSIE with each NV.

The message transmitted is also used to obtain the direction, speed and time information of each NV. Since NV2NV communication process including 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 6.6 with the dark black lines. The probability analysis of the proposed scheme ESATRM will be determined subsequently below. For now, it is important to determine the ESATR as follows: In Figure 6.6, the area of the elliptical segment MON is determined as below:

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

Buy deductions, the area can be further simplified to:

$$\frac{ab}{2} (\alpha - \beta) - \frac{b}{a} \left( \frac{a^2}{2} \sin(\alpha - \beta) \right) = \frac{ab}{2} ((\alpha - \beta) - \sin(\alpha - \beta)) \quad (3)$$

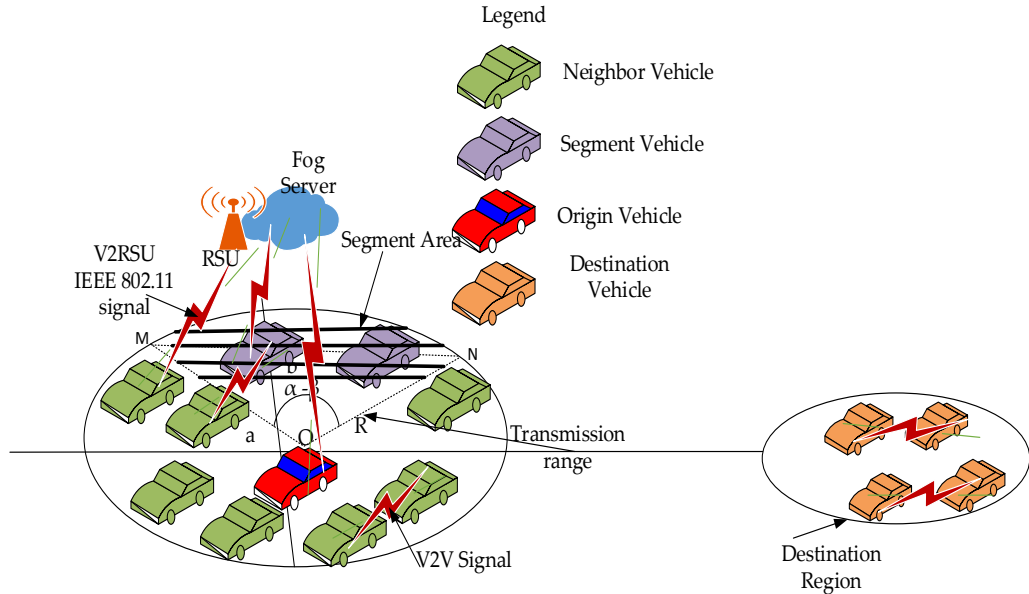


Figure 6.6: Vehicles in Elliptical Segment Transmission Range Model (ESATRM)

Figure 6.6 also demonstrates the movement of vehicles in the designated PESATRM. The PESATRM utilizes maximum transmission range. It is based upon specified NV relationship with each other NV. Based upon this, each NV are required to transmit IEEE 802.11p beacons hello message with each other NV. The NV 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 hybrid DoS attacks (HDSA) and all forms of attack which occur at different: speed, direction and time. 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.

## 6.6.1 Fog Server (FS) Further Authentication Process in Elliptical

### Segment Area

The models encompass PSAM and PESATRM. These models utilize FS and RSU for further authentication process. This is in order to ensure safe arrival of NODV that travels in the same ESA. The authentication process involves two fold performances. In the first performance, V2V communications are authenticated with each 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 ensure 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 RSA public key deployment is important. This include utilizing the common Gk as each NODV public key.

Each NODV vehicle/node is also required to pass RSA 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, which also utilize the following assumption that are important for the FS and RSU further authentication process of the PESARTM integration with SAM models as follow:

- FS and RSU message authentication denote VANET safety message announcement as standardized.

- PSAM integration with the PESATRM utilize the FS parameters which include:  $G_k, C, T$  where  $G_k$  is global public key of sender vehicle or NODV,  $C$  is  $Cert_{Xn}$  ( $n$  denotes possible pseudonym of vehicles of entity  $X$ , whereby one is also pseudonym of NODV and others are collected pseudonyms of other NV, and  $T$  denotes the authentication tag in the integration of PSAM and PESATRM which is installed through RSU and the FS.
- Based upon each possible signer vehicle which occur in the PESATRM, a validation  $\sigma_X$  is important. Where  $\sigma_X$  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 authentication algorithm are as follow:

---

**Algorithm 6.6:** Fog Server Further Authentication Algorithms for Proposed Models

---

1. Neighbor vehicle  $A$  (NVA) sends authenticated safety message (ASM) and share  $G_k$  through an initial broadcast/multicast and finally unicast to all vehicles within same ESATR, based upon the advocated scheme. Assume neighbor Vehicle  $B$  (NVB) is in the same ESATR that also represent 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  $K$ . Also send resulting ciphertext through the PSAM and PESATRM parameters

2. **if**  $NVB \rightarrow NVB : G_k, C, T$  **then**
3. set  $E_{Gk}(Cert_{NVB1}, \dots, Cert_{NVBn}, x_{NVB1}, \dots, x_{NVBn}, \sigma_{NVA})$
4. **If**  $NVA \rightarrow NVB$  **then**
5. set  $E_{Gk}(Cert_{NVA1}, \dots, Cert_{NVA n}, x_{NVA1}, \dots, x_{NVA n}, \sigma_{NVB})$
6. **end if**
7. **end if**
8. **end if**
9. **end**

In the second performance, further FS and RSU authentication process are employed. Each V2V communication process utilizes and transmits IEEE 802.11 beacons for SRSIE. This takes place so that each NODV can also share and utilize SRSIE amongst themselves. This performance process employs 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, requires an exchange of application-specific trustworthiness data. It utilizes the secure  $G_k$  sharing. Thus, the data exchanges must first ensure that it has been protected from any form of DoS JSA NODV, which does not use the application. This enable 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 to exchange SRSIE with each other accurately [88].

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

### **6.6.2 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 include utilization of NSHV concept of authentication based upon the FS and the RSU authentication algorithm, and secure SRSIE. Based upon this, NSHV links are set up for forwarding packets. It utilizes the transmission and relay of IEEE 802.11p beacons in the ESATRM, based upon NV to NV, utilized in the communication process. Based upon this, a sender  $NV_A$  is required to find at least the NSHV  $NV_B$  which is in the same ESATR. This follows with authentication and subsequent transmission of the SRSIE, based upon the PESATRM deployment. NV/ NODV which are present in ESATRM utilize three parameters including: density  $\lambda$ , segment angle  $(\alpha - \beta)$ , and transmission range  $R$ .

The PESATRM probability analysis has an objective of analyzing the impact of the parameters  $\lambda$ ,  $(\alpha - \beta)$  and  $R$ . In addition, the PESATRM is also anticipated for use where it is also important for providing secure authentication, which secures each NV2NV

communication, based upon also sharing of  $G_k$  with individual NV. The objective of utilizing sharing of  $G_k$  that falls in the same ESATR also include the probability analysis of locating at least one NV for sharing of  $G_k$  in the segment area. This objective can be achieved when different values are assigned to  $(\alpha - \beta)$  in the increasing order, until a NODV is found in the ESATR that would authenticate and also share the common  $G_k$  with each other neighbor vehicles during the vehicle's movement of NODV in the ESATR.

The movement of NODV is considered to take place using two dimensional network area, 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 NV that are present in the ESATR is obtained using a Poisson distribution. In addition, each NODV arrival, also depends on how successful it is able to initially get authenticated, with each other NV. It is then followed with the secure sharing of the  $G_k$  with each other NODV vehicle and include exchange of the standardized safety and road emergency conditions with each driver or vehicles on the road.

The proposed scheme uses NODV position to initially broadcast/multicast and finally unicast information to other NV, which falls in the same ESATR. In addition, it is presumed that the proposed scheme PESATRM probability analysis also utilize the attacked packet detection algorithms that was achieved in the PSAM. This was in order to anticipate mitigating against all form of attacks and HDSA that may be encountered in the ESATR. The proposed scheme SAM which is already integrated with the PESATRM are also deployed together to prevent the network from malicious nodes to become part of the

network. The NODV position information is represented through both  $x$  and  $y$  coordinates on a plane using 2D network model.

Optimal transmission range investigation for VANET has been conducted by various researchers [89-90]. In those studies, it was revealed that transmission range requirements in VANET decreases with increase in vehicle density. High density vehicular traffic situation requires smaller transmission range. Moreover, we recall that NV2NV communication would also require authentication/encryption of data, including the sharing of the Gk in a non-shadow environment (ENSE). The ENSE avoid real-time conflicting in transmissions of data authentication and exchange of information in shadow area, in which neighbor vehicles transmission would result in collision/congestion [91]. Therefore, we adopt our previous work in [92] proposed scheme ESATR detection process of DoS attacks method used in [92].

By referring to the efficient transmission range for NV, we chose a transmission range between (250m-550m). However, we consider the smaller transmission range of 250m as effective. This is because of reduced CO that can be utilized in the elliptical segment probability analysis of the NV/NODV. We consider  $X$  being random variable which represents the number of NV/NODV present and located in the ESATR, whereby each NV/NODV possess global key (Gk). After each NV/NODV gets authenticated and share the Gk securely, the probability  $P_{S_{area}}^{ENSE}(X = n)$  in the presence of  $n$  NV/NODV in the proposed ESATR which utilize encrypted SRSIE, in non-shadow environment (ENSE) can be obtained in the given Equation (4) as:

$$\begin{aligned}
& P_{S_{area}}^{ENSE}(X = n) \\
&= \frac{(\lambda \times S_{area})^n \times e^{-(\lambda \times S_{area})}}{n!}
\end{aligned} \tag{4}$$

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

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

$$\begin{aligned}
P_{S_{area}}^{ENSE}(X = 0) &= \left[ \frac{\left[ \lambda \left\{ \frac{ab}{2}(\alpha - \beta) - \frac{b}{a} \left( \frac{a^2}{2} \sin(\alpha - \beta) \right) = \frac{ab}{2}((\alpha - \beta) - \sin(\alpha - \beta)) \right\} \right]^0}{0!} \right] \times \\
&e^{-\lambda \left\{ \frac{ab}{2}(\alpha - \beta) - \frac{b}{a} \left( \frac{a^2}{2} \sin(\alpha - \beta) \right) = \frac{ab}{2}((\alpha - \beta) - \sin(\alpha - \beta)) \right\}} \\
P_{S_{area}}^{ENSE}(X = 0) \\
&= e^{-\lambda \left\{ \frac{ab}{2}(\alpha - \beta) - \frac{b}{a} \left( \frac{a^2}{2} \sin(\alpha - \beta) \right) = \frac{ab}{2}((\alpha - \beta) - \sin(\alpha - \beta)) \right\}}
\end{aligned} \tag{6}$$

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

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

The above PESATRM probability analysis model, which integrates with the PSAM, have been proposed in addition to message broadcast algorithms that were

investigated. These have been used to decrease the broadcasting storm in the network. Moreover, the model's integration has reduced trustworthiness concern in the network. The combined effect of the PESATRM and algorithms have also increased establishing trust in the network. This was possible through achieved efficient ESATR. In addition, the algorithms implemented in the proposed scheme models ESATRM and SAM, have also lessened the iterated broadcasting to keep less overhead of the information, and decrease the network load.

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

**Table 6.6: Cuckoo/CSA (ABC) Specification**

---

<b>CSA population</b>	Total number of vehicular nodes in the coverage elliptical segment region
-----------------------	---

<b>Fitness parameters Feedback</b>	of probability of new vehicles as part of the network, $V_i^k$
------------------------------------	--

fitness value

---

To determine Fitness value =  $V_i^k$  (8)

where  $V$  is vehicular node,  $k$  is evolved from initial point ( $k = 0$ ) to total gen iteration number, Cuckoo/CSA (ABC) has a powerful feature to generate new candidate vehicles/nodes solution to be part of the network. Based upon that approach, a new candidate solution  $V_i^{k+1}$  ( $i \in [1 \dots, N]$ ) is produced through disturbing the current  $V_i^k$  with a position change  $p_i$ .  $N$  is the number of vehicular nodes in the network. To obtain  $p_i$ , random step  $s_i$  is generated through symmetric Levy distribution using an algorithm in [93].

Finally, the solution for new vehicular nodes solution,  $V_i^{k+1}$  is obtained using:

$$V_i^{k+1} = V_i^k + p_i \quad (9)$$

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

The operation can be done with the following model:

$$V_i^{k+1} = \begin{cases} V_i^k + \text{rand.} \cdot (V_{r_1}^k - V_{r_2}^k) & \text{with probability } P_a \\ V_i^k & \text{with probability } (1 - P_a), \end{cases} \quad (10)$$

Where rand is a random number normally distributed, and  $r_1$  and  $r_2$  are random integers

from 1 to  $N$

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

The procedure can be done through the following statement:

$$V_i^{k+1} = \begin{cases} V_i^{k+1}, & \text{if } f(V_i^{k+1}) < f(V_i^k) \\ V_i^k, & \text{otherwise.} \end{cases} \quad (11)$$

This Cuckoo/CSA (ABC) selection strategy demonstrate that only high quality vehicular nodes which utilizes relay of high IEEE 802.11p signal associated (best solution near the optimal value) have the opportunity to interact with the RSU and the FS to deliver emergency feedback information like accidents and bad road condition to alert road users.

After the selection of the legitimate nodes 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.

## 6.7 Trust Provision in the Proposed Scheme

In order to provide trust in the network, it is anticipated that all other forms of attacks including hybrid DoS attack (HDSA) that may be hard to detect in the proposed scheme models: HDAM, PSAM and PESATRM, has one solution that can also be devised is to evaluate the probability information received through a consensus mechanism [94]. Thus, false information reaction due to the HDSA and other attack would require a vehicle to wait for receiving a given information based upon binary numbers (ones and zeroes). Let

us consider a vehicle that transmits the information/message and during the transmission, a DoS attack including all forms of attacks occurs because of the neighboring vehicles that disturb or amends 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 takes a decision whether the driver should consider the message as trusted on 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 [95].

$$Vechile_{trust} = \sum \text{number of ones} \quad (12)$$

To decide how instant the receiving vehicle would trust the vehicle which transmits the message to the base station, RSU and FS, the following equation has been used:

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

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 receiver with the access points and vehicles,  $t(ap\&S)$  is the time of transmission and receiver with the access points and server,  $t(s\&frv)$  is the time of transmission and receiver with the fog server and feedback of reporting vehicles and  $t(p)$  is the server's processing time [96]. In the proposed scheme PSAM, the communication ranges from (250-500)



meters and the information is transmitted at 30Mbps [97]. Therefore, the transmission time can be determined by using the following equation:

$$\text{Time} = \frac{\text{Distance}}{\text{Speed}} \quad (14)$$

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

$$d = \sqrt{(y_m - y_n)^2 + (x_m - x_n)^2} \quad (15)$$

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

### 6.8 RSU Network Prevention Mechanism Against Hybrid DoS attacks

The network construction is done with the following specifications:

Table 6.8. Network Specifications

---

total number of vehicles	60-100
the height of the network	1000m
the width of the network	1000m
node displacement	150-500m/s
simulation iterations	1500
simulation tool	matlab
encryption technique	VEHICULAR RSA
MAC/PHY	802.11p

---



---

#### Algorithm 6.8 (a): Random Vehicle Positioning (Total Vehicles)

---

// for uncertainties in the network, the network is placed in a random position manner

1. **for** each n in Nodes/vehicles
  2. X pos (n) =1000\*rand //creating a random x coordinate
  3. Y pos (n) =1000\*rand//creating random y coordinate
  4. Place (Xpos (n), Ypos (n))// Placing the node in their position in the network
  5. **end for**
  6. **end**
- 

#### **Algorithm 6.8 (b): Random delay detection in Vehicles**

---

1. **For** i=1: Vehicle/Nodes // Loop running for each node
  2. Set End2End Delaying (i) =Random; // Putting an end-to-end delay value for node acting normal
  3. End2End Delay (i) =(End2End Dealy\_n)<sup>2</sup>; // now, the expected reality is unpredictable and hence just for the random //architecture is set to be square of the normal delay
  4. **End for**
  5. **End**
- 

As the end2end delay is initialized, in the similar fashion the other parameters like jitter, packet drop, jamming signal resources consumption/RSU, CPU overutilization, and all other forms of anticipated DoS attacks in the network performance metric parameters are also initialized. In VANET, we envisage that there is no excessive battery consumption, due to the fact that as the vehicles in the communication process keeps moving, in order to determine the end2end 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 little different structure. Networks do not have any fixed structure, nevertheless, for any simulation there are parameters which should be initialized.

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

### 6.8.1 Modelling of all DoS Threat Prevention

This dissertation focuses on the prevention of all forms of DoS attack. The architecture of all forms of DoS is as follows.

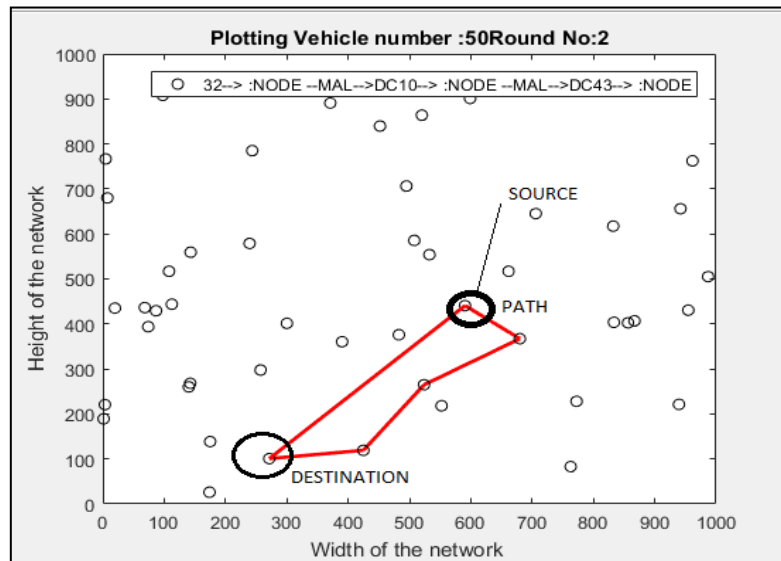


Figure. 6.8.1 (A) Vehicle Path Constructed

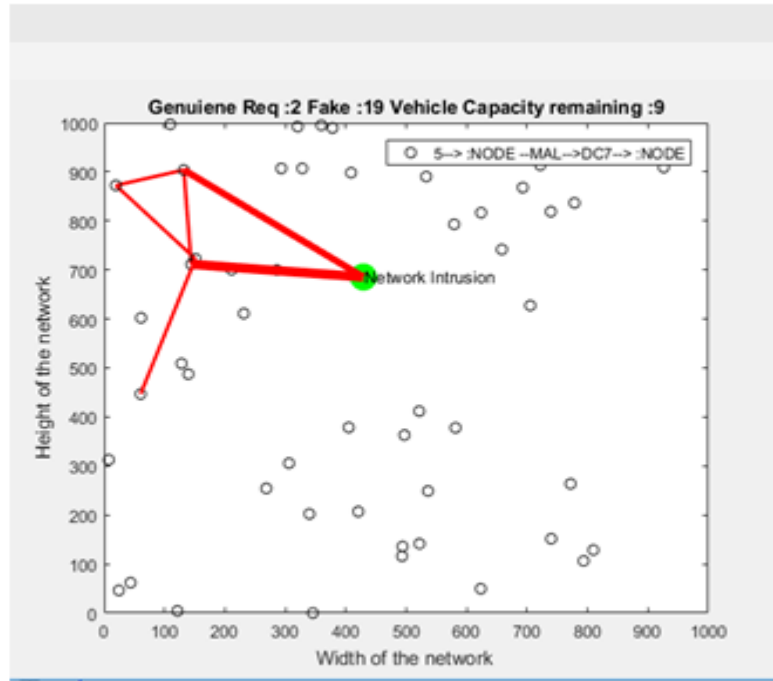


Figure 6.8.1 (b): Malicious node/ DoS Attackers

Figure 6.8.1 (a) and 6.8.1 (b) represents the path construction and the malicious network DoS mode of the attackers respectively. Figure 6.8.1 (b) shows that the intensity of dumping end2end delayed packet of the various DoS attacker such as jamming signal, packet drop, and resources consumption/CPU overutilization etc. varies at different instances of time. If the intensity of all these forms of DoS attackers and others are high, obviously the attackers are attempting to dump more packets which results in more packet drop, jamming signal and resources consumption/RSU and CPU overutilization etc. which might affect the RSU for prolonged end2end delay in the network. Based upon this, we define the following equation:

$$T_{pd} = P_{dn} + P_{da} \tag{16}$$

$T_{pd}$  is total packet drop,  $P_{dn}$  is the total number of dropped packets in normal mode and  $P_{da}$  is packet dropped when the network is under threat, which experienced all types of DoS attacks. In addition, we also define the following equation in relation to the types of the attacks as:

$$P_{dr} = (T_p - T_{pd}) / T_p \quad (17)$$

$P_{dr}$  is packet delivery ratio and  $T_p$  is 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 solution utilizes FFBP-NN and the general functions of FFBP-NN are as follows:

Table 6.8.1. .FIRELY USED 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) is 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 training process and Classification/optimization process. In the training process we utilized jitter as the training parameter to train the neural network using the MATLAB neural network toolbox. 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 all forms of attacks including hybrid DoS attacks based upon the communications experience of vehicles through the transmission of IEEE 802.11p. And then in the second process, the training is done for identifying the vehicles on the route that were also affected by all forms attacks including the hybrid DoS attacks.

The classification/optimization process optimizes the real-time signal timings during a given attacks situation, including hybrid DoS attack traffic which is due to congestion/jamming signal, packet drop, resources consumption/RSU overutilization situation.

Equation (18) below can be defined for the end2end jitter based upon AI processes as follows:

$$Jitr = E2EDP(at, nt) + Ntd \quad (18)$$

From equation (18), Jitr is the jitter, E2EDP is the end2end delay of the path, 'at' and 'nt' represents 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 first 450 to 600 iteration data for training and then for the next 650 iterations and above for training

the structure for identification of the path delayed in vehicles communication process based upon the proposed .

TABLE 6.8.2: FURTHER ACRONYMS

<b>Notation</b>	<b>Description</b>
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 6.8.1: Train\_Neural (Reiteration Data, Total Reiterations)**

---

1. **for** i=1:Total\_Reiterations
  2. setTraining\_Data (i) =Reiteration\_Data (i) **then**
  3. Target\_Label (i) =Path\_ID;
  4. **end for**
  5. Neural=Initialize\_Neural (Training\_Data, Target\_Label, k); // k is Total Neurons (40 in proposed case)
  6. Neural.TrainParam.Epochs=140;//total training iterations
  7. Train (NeuralTraining\_Data, Target\_Label); //training with Initialized Neural and Training data
  - 8. end**
- 

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



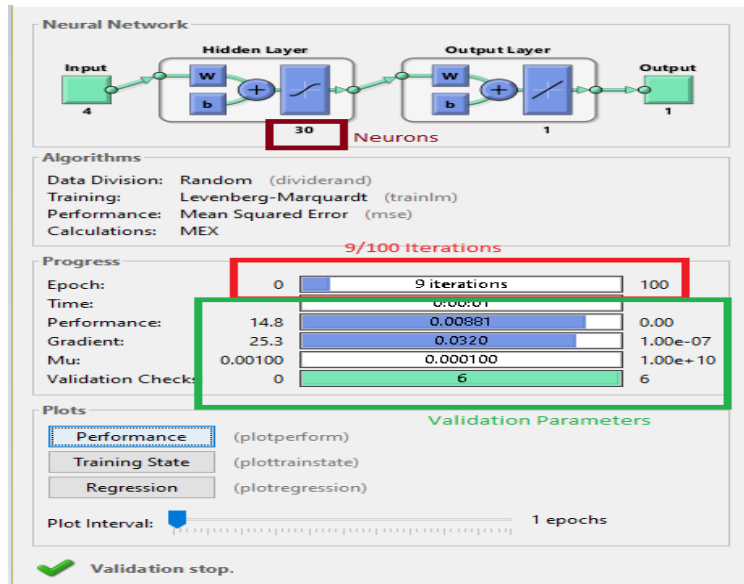


Fig. 6.8.1.2(a) Feed Forward propagation Structure

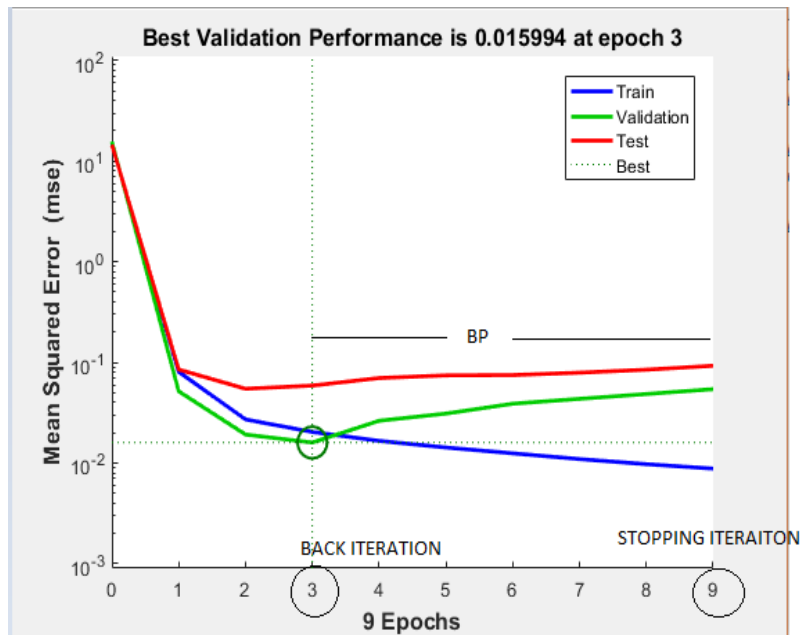


Fig 6.8.1.2 (b) Back Propagation Firefly

## 6.8.2 Identification of all affected Node and Retrieval

The proposed research work scheme also presents a regression model with the back propagation .as shown in figure 6.8 .2

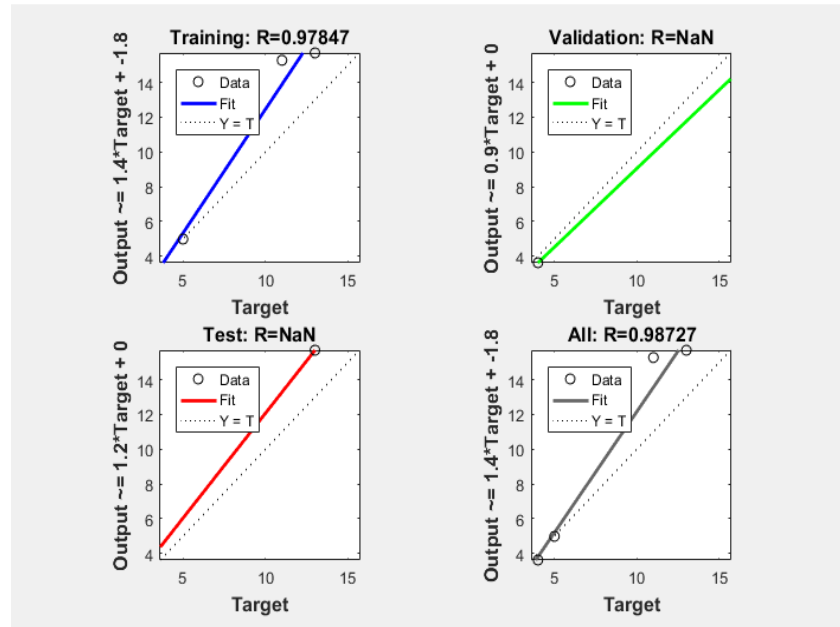


Figure 6.8.2 Regression Model

Figure 6.8.2 represents close but least /high regression values of the proposed scheme. These results show detail regression model that was generated in the simulation before the final regression values were obtained. The result generated includes the following: The training result is 0.97847, the validation result is Nan (not a number), the test result is NaN, and the value for all result is 0.98727. Close and least/high regression values generally represent healthy training and classification structure as well, as indicated previously.

## 6.9 Results analysis and discussion

Figure 6.8.1.2b illustrate the back propagation Firefly graph. Based upon the graph, the proposed scheme and the models determines the training data jitter and also validates 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 6.8.1.2b, we can also realize that we have 9 epochs of the proposed scheme model, implying that the proposed scheme models are trained over 9 epochs as the forward iteration and 3 epochs for backwards iteration. We expect also that the proposed scheme models will also decrease with each epoch, meaning our model is predicting value y more and accurately as the model is further continued for training. The test graph also indicates that validation performance at epoch 3 the prediction of the proposed model is a good one.

From Figure 6.8.2, regression model of the proposed scheme is evaluated. Based upon the evaluation, training result is 0.7847; validation result is NaN (not a number); test result is NaN, and all result is 0.98727. These values represent close but high regression values. Generally, close but high regression values represents healthy training and classification structure. High regression value is also the reason for which the prevention parameters of all forms of DoS activities causing jitter/delay in the network falls high. As discussed earlier, this section classifies the path value on the basis of the trained structure. The identified malicious vehicle/node is always sent for recovery or maintenance. The following evaluations are also made.

### **6.9.1 Analysis of Jitter, Throughput and Prediction Accuracy of the proposed Scheme and the others**

Based upon the proposed scheme, comparison analysis is made with the other contending schemes such as: CUCKOO/Artificial Bee Colony (ABC) and Firefly/ Genetic algorithm (GA). We determined jitter, throughput and the prediction accuracy. Based upon this we evaluated end2end delay packet detection of all form attacks including hybrid DoS attacks observed in the paths of vehicles traveling in the network and communicated. We utilized the simulation with the packet detection algorithms including unicast and multicast/broadcast data transmission utilizing a single next hop vehicle (SNHV) data transfer probability based upon the proposed scheme models: HDAM, and SAM integrated with ESATRM of the vehicles communications process which include: V2V, V2RSU and RSU2V through the IEEE 802.11p beacons transmissions in the network which is based upon DSRC technology.

Thus, the result of the proposed work scheme which include jitter, throughput and prediction accuracy is compared with the prevention done with CUCKOO (ABC) and Firefly (GA) protocols as follows.

### **6.9.2 Jitter Analysis**

Evaluating the Jitter, the proposed scheme jitter is based upon the end2end delayed path of the vehicles utilizing the proposed scheme models including HDAM, PSAM and the PESATRM communication process, which is 60ms at maximum. Whereas the jitter is 93ms with CUCKOO (ABC) and 89ms with Firefly (GA) respectively. This is because, the

proposed scheme architecture models utilized the training structure more efficiently and it does not have to compare the entire feature set which consumes a lot of time in the case of hybrid DoS threat detection, based upon the packet transmitted in the model's 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 below in Equation (19) as:

$$Avg_{jitter} = \frac{Max_{jitter} - Min_{jitter}}{2} \quad (19)$$

Table 6.9.2. 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

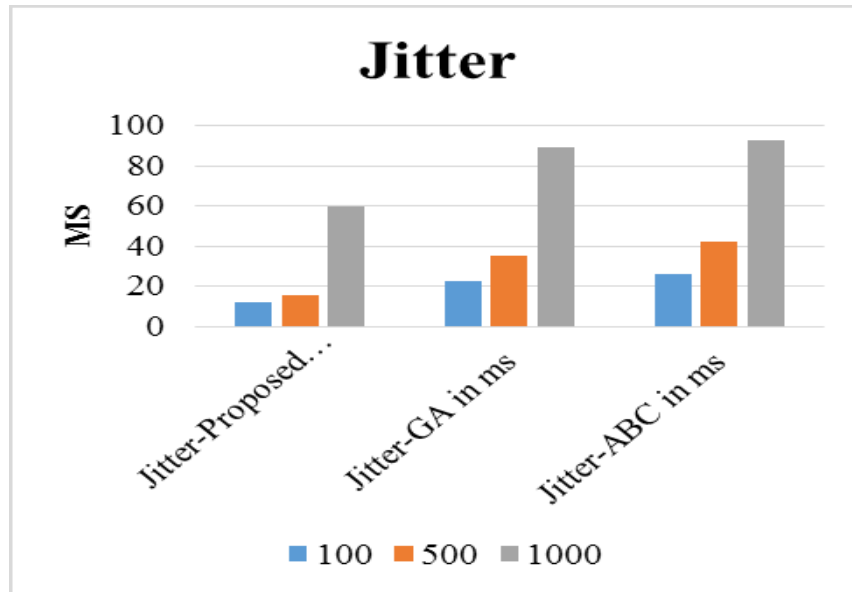


Figure 6.9.2: Jitter for Proposed Scheme versus other 2 Schemes

Table 6.9.3. Average jitter Value

<b>Proposed Jitter</b>	<b>Average</b>	<b>24</b>
<b>Firefly Average Jitter</b>		<b>33</b>
<b>CUCKOO Jitter</b>	<b>Average</b>	<b>33.5</b>

$$\% \text{ Improvement} = \frac{(Final * 100)}{Initial} \quad (19)$$

TABLE 6.9.4 TABLE OF PERCENTAGE JITTER IMPROVEMENT

<b>Proposed to FIREFLY</b>	<b>72%</b>
<b>Proposed to CUCKOO</b>	<b>71.64%</b>

### 6.9.3 Throughput Analysis

The second evaluation is done 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 by Equation (20):

$$\text{Throughput} = T_{dp} * t_m \quad (20)$$

$T_{dp}$  = Total delivered packets,  $t_m$  = total time of transmitting information from Transmitting vehicle/node to receiving vehicle/node in the proposed scheme SAM.

Table 6.9.5 Throughput

Iteration Count	Throughput-Proposed	Throughput-CUCKOO	Throughput-FIREFLY
100	523300	235411	365412
500	652311	352210	356221
1000	721112	396521	385211

### 6.9.4 Prediction Accuracy Analysis

The third evaluation is also done on the basis of the prediction accuracy of the proposed scheme and compared with the other contending schemes including: Artificial Bee Colony (CUCKOO) and Genetic Algorithm (Firefly) protocols. The prediction accuracy is also determined and shown in table 8 below as:

Table 6.9.6 Prediction Accuracy

Proposed Scheme	92%
CUCKOO	63%
FIREFLY	63.89%

The proposed scheme algorithms and models including HDAM, PSAM, and PESATRM utilizes maximum time which results in least end2end delay on the path of the vehicles jitter value. 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 CUCKOO (ABC) and the Firefly (GA) scheme and models.

Table 6.9.7: SUMMARY OF BACKGROUND STUDY COMPARISON OF VANET PROTOCOLS BASED ON TRUSTWORTHINESS, ATTACKS DETECTION AND MODE OF TRANSMISSION

<b>VANET Protocols</b>	<b>Data Transmission mode</b>	<b>Performance measurement for accuracy and trustworthiness</b>	<b>Attacks Detection</b>	<b>Storage and authentication Mechanism</b>



[9]	None	No trustworthiness and accuracy	Only DoS JSA	None
[10]	None	No trustworthiness and prediction accuracy	Only DoS JSA	None
[11]	Unicast traffic mode	No trustworthiness and prediction accuracy	Only DoS JSA	None
[12]	Broadcast traffic mode	No trustworthiness and prediction accuracy	Only DoS JSA	None
[14],[15][16] and [17]	None	No trustworthiness and prediction accuracy	Only DoS JSA	VFC only
Proposed scheme protocol	Unicast, broadcast/multicast	Trustworthiness and prediction accuracy	Hybrid of DoS JSA, PD, and RCRCO	VFC, OA, and KDE

## **CHAPTER 7: CONCLUSIONS AND FUTURE WORK**

This dissertation proposed a fog-integrated VANET scheme. The proposed scheme simultaneously considers the node level and network level security. The node level security includes the Fog computing merged with the VANET, a node level and network level security mechanism, new fitness function of the Cuckoo search, and a collaborated neural network structure. Both the node level and network level security establish trust collaboration with all the network neighbors. The node and the network level trustworthiness ensure that the entire network rapidly delivers packet in the entire network system. The proposed scheme also prevents DoS and SNI attacks from attacking the entire network. The proposed scheme is ad hoc, and a new vehicle identified with DoS and SNI may easily enter the network.

To prevent the network from being assessed by foreigners (outsiders), until they become part of the network, LaGrange interpolation method is used through which a node level and network level security attacks entry is secured

The proposed scheme also utilizes an integrated SAPM. The SAPM includes intrusion/attacker and VSIF models. Both models' deployment in SAPM are utilized to mitigate all other forms of attacks and secure the network. The models are also deployed to provide real-time information in the network through safety application deployment of

the RSU at the TMO, where information can be processed on timely to reduce delay and enhanced the throughput in the network. The evaluation of the proposed SIVNFC scheme is evaluated using QoS parameters—namely, the throughput and jitter. The proposed model is also compared with the firefly algorithm, a single neural network, a neural network combined with the firefly algorithm, and the Cuckoo Search algorithm.

The evaluation of the QoS parameters is done using the PIR as the basis of every simulation. The proposed scheme provided a total throughput of 8100 for the PIR value of 0.2. The maximum throughput of the network was also offered. For the same scenario, the second-best throughput was 7900 for the combination of Firefly and the neural network. The jitter is inconsistent throughout the simulations, and it varied based on the model architecture and algorithm. Even after nonlinear computations, the jitter for the scheme is a maximum of 96 ms, whereas it is 102 ms for the firefly neural network.

The maximum attained throughput for the proposed scheme is importantly high as compared to Cuckoo (ABC) and Firefly (GA). The dissertation utilized FFBP-NN over 100 iterations out of which 30-40 iterations are reserved for back propaFireflytion.

The proposed scheme also utilizes the regression model to indicate the reduced delay of the network. The current research work has potential for future research directions. The neural network structure can be varied to assess if there are any differences in the QoS parameters. A hybrid classifier can also be tested to see if it enhances the current proposed neural architecture. This dissertation utilized Lagrange's interpolation method, and it would be interesting to examine the performances of other interpolation methods such as Spline and the Polynomial fit. A combination of interpolation methods can also be

considered.

Vehicular ad hoc network (VANET), also has the main objective of benefiting from ITS (intelligent transportation system). It avoids heavy traffic condition and driving problems that may be encountered on the roads, including highways driving. Due to openness nature of VANET deployment a lot of trustworthiness issues, including hybrid DoS attacks (HDSA) and other forms of attacks can be predictable with VANET. This leads to sporadic process of information which prevents real-time information delivery of V2V communication, and therefore introduce end2end delay in the network. This requires secure, efficient storage delivery and trustworthiness solution. This research has also presented fog computing in cloud-based integration (VFC) concept for securing VANET. The research has also utilized hybrid optimization algorithms (HOAs) which are also intelligent and include: CSA/ABC, Firefly/GA.

These HOAs are heuristics which have problem solving skills. The HOAs, in addition to the network Vehicular authentication algorithms and further FS and RSU further authentication algorithms, have been used to select trustworthy nodes against HDSA and others. This has also secured the transmissions of IEEE 802.11p beacon relay in VANET, during V2V V2RSU communication etc. for delivery of V2V standardized road safety information exchange (SRSIE) using VANET Infrastructure Architecture (VIA). In this dissertation, the system architecture models of VIA and several interesting application scenarios, challenging issues of VFC for delivery of SRSIE in VANETs, in relation to HDSA attacked packet detection algorithms for VIA models have been proposed.

The proposed scheme VIA 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 for identifying and mitigating all forms of attacks including HDSA, DoS JSA and all other associated vulnerabilities, which utilized IEEE 802.11p beacons transmission relay in V2V information dissemination. Moreover, PSAM is the overall proposed scheme system model. PSAM utilizes attacked packet detection algorithms (APDA). APDA is used to identify the vehicle position, frequency based upon the number of attacked packet. It uses multicast/broadcast and unicast mode of transmission of data, utilizing the IEEE 802.11p beacons/signals for real-time data delivery.

The PSAM also integrates with the PESATRM to provide robustness in VIA deployment. This serves as an additional proposed models of the proposed scheme that utilize efficient ESATR to process the delivery of SRSIE. The PSAM and PESATRM integration models also provides further secure authentication and key distribution establishment (AKDE) in the RSU and the FS. This secures the network for trustworthiness PESATRM utilize probability analysis and also encompass NSHV and non-shadow environment encryption (NESE) concept of VFC communication. This provide secure and SRSIE to sensitize the vehicles which move in the same transmission range, in order to effectively prevent road casualties in timely manner.

VFC integration with HOA and AKDE supports rising VANET applications that demands predictable results with minimum energy consumption rate. This research has also focused on the dual training mechanism of Firefly (GA)/ FFBP-NN to provide

prevention and recovery mechanism for all malicious nodes path detection for end2end delay path observed in the VANET. It also includes reduced jitter for the proposed scheme significantly. As a result, the detection and prevention of all forms of attacks including HDSA stands high. Based upon this, the proposed scheme prediction accuracy is 92%. The proposed scheme uses the concept of authentication /encryption and trustworthiness of nodes. The network provision also utilizes hybrid information broadcast/multicast and unicast in the VANET.

However, compared to Cuckoo (ABC) and Firefly (GA), their prediction accuracy is respectively 63% and 63.89%. These schemes have limitation in trustworthiness provision in VANET. They do not usually include HOAs and A KDE. In addition, the proposed scheme algorithm and the models which include HDAM, PSAM and PESATRM, have significantly contributed efficiently to reduce 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 dissertation also utilized FFBP-NN over 100 iterations out of which 30-40 iterations are reserved for back propaFireflytion.

The current scenario opens a lot of future work approaches. In our future work, we would like to design the layout and implementation of VANET with all other forms of optimization technique which include using Spline method, to minimize the jitter problems in fog computing environment, in order to asses performance based upon different forms of attacks scenarios in the network.

## REFERENCES

1. Shankar Yadav, Ranvijay, Dinesh Singh. “A state-of-art approach to misbehavior detection and revocation in VANET: Survey”. International. Journal. Ad Hoc Ubiquitous Computing. January **2018**, Vol. 28, pp. 77–93.
2. Craig Cooper, Daniel Franklin , Montserrat Ros, Farzad Safaei and Mehran Abolhasan. “A comparative survey of VANET clustering techniques”. IEEE Communication Survey, 2017, Vol. 19, pp. 657–681.
3. Hamssa Hasrouny, Abed Ellatif Sahat, Carole Bassil and Anis Laouit. “VANET Security challenges and solutions”: A survey. Vehicular. Communications. January **2017**, Vol 7, pp. 7–20.
4. Sharma Sharma, and Ajay Kaul. “A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud”. Vehicular. Communication. April **2018**, Vol 12, pp. 138–164.
5. Ramu Panayappan, Trivedi Jayin mukul Trivel , Aren Studer and Adrian Perrig. “VANET-Based Approach for Parking Space Availability”, Carnegie Cylab Mellon University: Pittsburgh, PA, USA, 2007; pp. 1–4.
6. Jyoti Grover, Ashish Jain, and Sunita Singhal. “A. Real-Time VANET Applications Using Fog Computing”. In Proceedings of the First International Conference on Smart System, Innovations and Computing, Smart Innovation, Systems and Technologies, Jaipur, 2018;

- pp. 685–687.
7. Steve Glass, Imad Mahgoub, and Monika Rathod. “Leveraging MANET-Based Cooperative Cache Discovery Techniques in VANETs: A Survey and Analysis”. *IEEE Communication. Survey*. May **2017**, Vol. 19, pp. 2640–2661.
  8. Sanya Chaba, Rahul Kumar, Rohan Paint, and Mayank Dave. “Secure and efficient key delivery in VANET using cloud and fog computing”. In *Proceedings of the International Conference on Computer, Communications and Electronics (Comptelix)*, July 2017, pp. 27–31.
  9. Calandrelli, G.; Papadimitratos, P.; Hubaux, J.-P.; Lioy, A. *Efficient and Robust Pseudonymous Authentication in VANET*; Laboratory for Computer Communications and Applications, EPFL: Lausanne Switzerland, 2007; pp. 19–23.
  10. Ruifang Li, and Lisha Jin. “Improved Cuckoo Algorithm for Spectrum Allocation in Cognitive Vehicular Network”. In *Proceedings of the 2018 5th International Conference on Systems and Informatics (ICSAI 2018)*, Nanjing, China, November 2018. pp. 823–833.
  11. Ruining Zhang, Xuemei Jiang, and Rufing Li. “Decomposition based multi-objective spectrum allocation algorithm for cognitive vehicular networks”. In *Proceedings of the IEEE 17th International Conference on Communication Technology (ICCT)*, Chengdu, China, October 2017; pp. 1–3.
  12. Narawade Kolekar, “Decomposition based multi-objective spectrum allocation algorithm for cognitive vehicular networks. In *Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, February 2017; pp. 715–720.
  13. Freeha Azmat, Yunfei Chen, Nigel Stocks. “Analysis of Spectrum Occupancy Using



Machine Learning Algorithms”.

IEEE Transaction. Vehicular Technology. **2016**, Vol. 65, pp. 6853–6854.

14. Akansha Sachdev, Komal Mehta, Malik Letash. “Design of Protocol for cluster based routing in VANET using Firefly Algorithm”. In Proceedings of the 2016 IEEE International Conference on Engineering and Technology (ICETECH), Coimbatore, March 2016; pp. 1–3.
15. Rajesh Kumar, and Sahil Chhabra. “Efficient routing in Vehicular Ad-hoc Networks using Firefly optimization”. In Proceedings of the 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, August 2016 Vol 3; pp. 1–6.
16. Fuad A. Ghaleb, Anazid Zainal, Murad A. Rassam, Fathey Mohammed. “An effective misbehavior detection model using artificial neural network for vehicular ad hoc network applications”. In Proceedings of the 2017 IEEE Conference on Application, Information and Network Security (AINS), November 2017, pp. 1–5.
17. Yash Agarwal, Krtika Jain, and Orkun Karabasoglu. “Smart vehicle monitoring and assistance using cloud computing in Vehicular Ad Hoc networks”. International. J. Transp. Science. Technology. March **2018**, Vol. 7, pp. 60–73.
18. Ahmed Farhan, Muhammad Kazim, Asma Adnane, and Abir, Awad. “Vehicular Cloud Networks Architecture, Applications and Security Issues”. In Proceedings of the IEEE/ACM. International Conference on Utility and Cloud Computing (UCC), Limassol, December 2015, Vol 8 , pp. 571–576.
19. Rajamanickam Vennila, Veerappan Duraisamy. Inter cluster communication and rekeying technique for multicast security in mobile ad hoc networks. IET Information Security. Vol. 8, June **2014**, Vol 8, pp. 234–239.

20. Jian Kang, Dan Lin, Wei Jiang, and Elisa Bertino. "Highly efficient randomized authentication in VANETs". *Pervasive Mobile Computing*. February **2018**, Vol 44, pp. 31–44.
21. Dalya, K. Sheet, Omprakash Kaiwartya, Abdullah H. Abdullah, Ahmed Hassan. "Location Information Verification cum Security using TBM in Geocast Routing". In *Proceedings of the International Conference on Eco-Friendly Computing and Communication Systems*, December 2015, Vol 70, pp. 219–221.
22. Kashia Naser Qureshi, Abdul Hanan Abdullah, Omprakash Kaiwartya, Saleem Iqbal, Rizwan Aslam Butt, and Faisal Bashir. "A Dynamic Congestion Control Scheme for safety applications in vehicular ad hoc networks". *Computer and Electrical. Engineer* .November **2018**, Vol. 72, pp. 774–788.
23. Reena Kasana, Sushil Kumar, Omprakash Kaiwartya, Wei Yan, Yue Cao, and Abdul Hanan Abdullah. "Location error resilient geographical routing for vehicular ad-hoc networks". *IET Intelligent. Transportation. System*. **2017**, Vol. 11, pp. 450–452.
24. Dora Prasada Durga, Sushil Kumar, Omprakash Kaiwartya, and Shu Prakash. "Secured Time Stable Geocast (S-TSG) routing for VANET". In *Proceedings of the International Conference on Advanced Computing, Networking and Informatics, Smart Innovation, Systems and Technologies*, June 2015, Vol. 44, pp. 161–162.
25. Omprakash Kaiwartya, Yue Cao, Jamie Lloret, Sushil Kumar, Nuaman Aslam, and Rupale Kharel, "Geometry-based Localization for GPS Outage in Vehicular Cyber Physical Systems". *IEEE Transaction. Vehicular Technology*. May **2018**, Vol 67, pp. 3800–3801.
26. Shrikant Tangade, Sunil Kumar S. Manvi, Pascal Lorenz. "Decentralized and Scalable Privacy-Preserving Authentication Scheme in VANETs". *IEEE Transaction. Vehicle*.

- Technology. **2018**, Vol 67, pp. 8647–8655.
27. Yongxuan Lai, Lu Zhang, Tian Wang, Fan Yang, and Yifan Xu. “Data Gathering Framework Based on Fog Computing Paradigm in VANETs”. In Proceedings of the Asia-Pacific Web (APWeb) and Web-Age Information Management (WAIM) Joint Conference on Web and Big Data. July 2017, Springer 2017, pp. 227–236.
  28. Mohamed Shehab, Abdul Khader, Mohammed Azim Al-Betar, and Ahmad Tajudin. “A survey on applications and variants of the cuckoo search algorithm”. Applied. Software Computing. **2017**, Vol 61, pp. 1041–1059.
  29. Dan Liao, Hui Li, Gang Sun, Ming Zhang, and Victor Chang. “Location and trajectory privacy preservation in 5G-Enabled vehicle social network services”. Journal of Network and Computing. Application May. **2018**, Vol 110, pp. 108–118.
  30. Neha Kushwah, and Abhilash Sonker. “Malicious Node Detection on Vehicular Ad-Hoc Network Using Dempster Shafer Theory for Denial of Services Attack”. 2016 IEEE International Conference on Computational Intelligence and Communication Networks. Pp 432-433.
  31. Paramijt Singh Waraich, and Neera Batra. “Prevention of Denial of Service Attack over Vehicle Ad hoc Networks using Quick Response Table”.2017 IEEE International Conference on Signal processing, Computing and Control (ASPCC). Pp 586-587.
  32. Hichem Sedjelmaci, Sidi Mohammad Senouci S, and Mosa Ali Abu-Rghef. “An Efficient and Lightweight Intrusion Detection Mechanism for Service-Oriented Vehicular Networks”. IEEE 2014 Internet of Things Journal, 2014 Vol 1. Pp 570-571.

33. Munazza Shabbir, Muazzam Khan, Umair Shafiq Khan, Nazar A. Saqib. "Detection and Prevention of Distributed Denial of Service Attacks in VANETs". IEEE2016 International Conference on Computational Science and Computational Intelligence. pp 970-971.
34. Sparsh Sharma, & Ajay Kaul. "Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized IDS for VANET". Vehicular Communications, April 2018, Vol. 12, pp. 23-38.
35. Qi Jiang, Jianbin Ni, Jianfeng Ma, Li Yang, & Xuemin Shen. "Integrated Authentication and Key Agreement Framework for Vehicular Cloud Computing". IEEE 2018 Network, Vol. 32(3), pp. 28-35.
36. Yash Agarwal, Kritika Jain, & Orkan Karabasoglu. "Smart vehicle monitoring and assistance using cloud computing in vehicular Ad Hoc networks". International Journal of Transportation Science and Technology, Vol 7(1), pp. 60-73.
37. Steve Glass, Imad Mahgoub, & Monika Rathod. "Leveraging MANET-Based Cooperative Cache Discovery Techniques in VANETs: A Survey and Analysis". IEEE 2017 Communications Surveys & Tutorials, Vol 19(4), pp. 2640-2661.
38. Sanya Chaba, Rahul Kumar, Rohan Pant, & Mayank Dave. "Secure and efficient key delivery in VANET using cloud and fog computing. In Computer, Communications and Electronics (Comptelix), July 2017 IEEE International Conference, pp. 27-31.
39. Mendi Sookhak, F Richard Yu, & Helen Tang. "Secure data sharing for vehicular ad-hoc networks using cloud computing." In Ad Hoc Networks, Springer 2017, pp. 306-315.
40. Rajesh Kumar, & Sahil Chhabra. "Efficient routing in Vehicular Ad-hoc Networks using Firefly optimization". IEEE 2016 International Conference on Inventive Computation Technologies (ICICT). pp 1-6.

41. Mohammed E Amine Fekair, Abderrahman Lakas, and Ahmed Korichi A. "CBQoS-Vanet: Cluster-based Artificial Bee Colony Algorithm for QoS Routing Protocol in VANET". IEEE International Conference on Selected Topics in Mobile & Wireless Network (MoWNeT). April 2016 pp 1-3.
42. Mohammed Khalil, & Marianne A. Azer. "Sybil attack Prevention through Identity Symmetric Scheme in Vehicular Ad hoc Networks". IEEE 2018 Wireless days (WD). Pp 184-185.
43. S. Roselin Mary, M. Maheshwari, & M. Thamaraiselvan." Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)", 2013 IEEE International Conference on Information Communication and Embedded Systems (ICICES). pp 237-240.
44. Karen Verma, & Halabi Hasbullah."IP-CHOCK (filter)-Based Detection Scheme for Denial of Service (DoS) attacks in VANET. IEEE, 2014. 2014 International Conference Computer and Information Sciences (ICCOINS).pp 1-6.
45. Parmjit Singh Waraich, & Neera Bart. "Prevention of denial of service attack over vehicle ad hoc network using quick response table". In Proceedings of the 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), September 2017; pp. 568–589.
46. Miao Wang, Hao Liang, Ruilong Deng, Ran Zhang, & Xuemin Sheman Shen. "VANET based online charging strategy for electric vehicles". In Proceedings of the 2013 IEEE Global Communications Conference (GLOBECOM), December 2013; pp. 4804–4809.
47. Giulio Ministeri, & Lorenzo, Vangelista. "On the performance of channel occupancy detectors for vehicular ad-hoc networks". In Proceedings of the 2013 IEEE 5th

International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), September 2013; pp. 1–6.

48. Ayonija Pathre, Chetan Agrawal, & Aurag Jain. “A novel defense scheme against DDOS attack in VANET”. In Proceedings of the 2013 IEEE Tenth International Conference on Wireless and Optical Communications Networks (WOCN) July 2013; pp. 1–5.
49. Salim Bitam, & Abdelhamid Mellouk, A. “Bee life-based multi constraints multicast routing optimization for vehicular ad hoc networks”. *Journal of. Network and. Computing. Application.* **2013**, Vol 36, pp. 981–991.
50. Pathre, A. Identification of malicious vehicle in vane environment from DDOS attack. *J. Glob. Res. Comput. Sci.* **2013**, 4, 30–34.
51. Md Whaiduzzaman, Mehdi Sookhak, Abdulah Gani, and Rajkumar Buyya. “A survey on Vehicular cloud computing”. *Journal of. Network Computing Application* April. **2014**, Vol 40, pp. 325–344.
52. Jian Liu, Jiangtao Li, Lei Zhang, Fefei Dai, Yuanfei Zhang, X. Meng, X & Jiang Shen. “Secure intelligent traffic light control using fog computing”. *Future Generation Computing System.* **2018**, Vol 78, pp. 817–824.
53. Mehdi Sookhak, F. Richard Yu, & Helen Tang. “Secure data sharing for vehicular ad-hoc networks using cloud computing”. In Proceedings of the Ad Hoc Networks, June 2017; Springer 2017; pp. 306–315.
54. Jerferson Campos Nobre, Allen M. de Souza, Denis Rosário, Christiana Both, Leandro A. Villas, Eduardo Cerqueira, & Mario Gerla. “Vehicular software-defined networking and fog computing: Integration and design principles”. *Ad Hoc Network.* **2019**, Vol 82, pp. 172–181.

55. Ashish Rauniyar, Desta Haileselesie Hagos, & Manish Shrestha. “A Crowd-Based Intelligence Approach for Measurable Security, Privacy, and Dependability”. *Internet of Automated Vehicles with Vehicular Fog. Mobile Information System* **2018**, Vol 2018, pp. 828–829.
56. Ying He, Zhexieng Wei, Guingzheng Du, Jian Li, Nan Zhao, & Hongxi Yin. “Securing Cognitive Radio Vehicular Ad hoc Networks with Fog Computing”. *Ad Hoc Sensor. Wireless Network January* **2018**, pp. 1–4.
57. S. Anbuchelian, S. Lokesh, Madhusudhanan Baskaran. “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)*, August 2016; pp. 233–238.
58. Jiangnan Wei, Xiojie Wang, Nan Li, Guomin Yang, & Yi Mu. “A Privacy-Preserving Fog Computing Framework for Vehicular Crowd sensing Networks”. *IEEE Access* **2018**, Vol 6, pp. 43776–43784.
59. Hafizul Islam, Mohammed S. Obaidat, Pandi Vijayakumar, P, Enas Abdulhay, Fagen Li, Chatanya Reddy. “A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs”. *Future Generation Computing System* July **2018**, Vol 84, pp. 216–227.
60. Revashi Sundarasekar, M. Thanjaivadivel, Gunersekaran Manogaran, Priyan Malarvizhi Kumar, R. Varatharajan, Naaven Chilamkurti, Ching-Hsien Hsu. “Internet of Things with Maximal Overlap Discrete Wavelet Transform for Remote Health Monitoring of Abnormal ECG Signals”. *Journal of Medical System* 2018, Vol. 42, pp. 228.
61. Rong Yu, Yang Zhang, Stein Gjessing, Wenlong Xia, Kun Yang. *Toward cloud-based*

- vehicular networks with efficient resource management. *IEEE Network* **2013**, Vol. 27, pp. 48–54.
62. Mahmoud Hashem Ezra, Thomas Owens, Qiang Ni, & Qi Shi. “Situation-Aware QoS Routing Algorithm for Vehicular Ad Hoc Networks”. *IEEE Transaction on Vehicular Technology* 2015, Vol. 64, pp. 5520–5522.
63. Dinesh Singh, Ranvijay, & Rama Shankar Yadav. A state-of-art approach to misbehavior detection and revocation in VANET: survey. *International Journal of Ad Hoc and Ubiquitous Computing* 2018, Vol. 28(2), pp. 77-93.
64. Craig Cooper, Daniel Franklin, Montserrat Ros, Farzad Safaei, & Mehran Abolhasan. “A comparative survey of VANET clustering techniques”. *IEEE Communications Surveys & Tutorials* 2017, Vol .19(1), pp. 657-681.
65. Hamas Hasrouny, Abed Ellatif Samhat, Carole Bassil, Anis & Laouiti. VANET security challenges and solutions: A survey. *Vehicular Communications* 2017, Vol. 7, pp. 7-20.
66. Sparsh Sharma, & Ajay Kaul. . A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud. *Vehicular Communications* 2018, Vol. 12, pp. 138-164.
67. Claudia Campolo, & Antonella Molinaro, “Multichannel communications in vehicular ad hoc networks: a survey,” *IEEE 2013 Communication. Magazine*. Vol. 51, no. 5, pp. 158–169.
68. Claudia Campolo, Antonella Molinaro, Alexey Vinel, and Yan Zhang. “Modeling prioritized broadcasting in multichannel vehicular networks,” *IEEE Transaction on Vehicular Technology* 2012. Vol. 61, pp. 687–701.
69. S. Anbuchelian, S. Lokesh, and Madhusudhanan Baskaran. “Improving Security in



- Wireless Sensor Network Using Trust and Metaheuristic Algorithms”. 2016 3rd International Conference on Computer and Information Sciences (ICCOINS).pp 233-238.
70. Konstantinos Pelechrinis, Marios Iliofotou, and Srikanth V. Krishnamurthy. “Denial of service attacks in wireless networks: the case of jammers,” *IEEE Communications Surveys and Tutorials* 2011, Vol. 13, pp. 245–257.
  71. Jin Tang, Yu Cheng, and Weihua Zhuang. “Real-time misbehavior detection in IEEE 802.11 based wireless networks: an analytical approach.” *IEEE 2014 Transaction Mobile Computing*, Vol. 13 pp. 146-158.
  72. Soufiene Djahel, Zonghoua Zhang, Farid Nait-Abdesselam, and John Murphy, “Fast and efficient countermeasure for MAC Layer misbehavior in MANETs,” *IEEE 2012 Wireless Communication. Letter*, Vol. 1, no. 5, pp. 540–543.
  73. Ali Hamieh, Jalel Ben-othman, and Lynda Mokdad L. “Detection of radio interference attacks in VANET,”*IEEE 2009 Global. Telecommunications Conference*, Pp. 1-5.
  74. Lyamin N., Vinel A., Jonsson M., and Loo J. Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks *IEEE 2014 communications letters*, Vol. 18, pp. 110-113.
  75. Kalashnikov V., Lee W., and Hong J. MAC Aggregation Resilient to DoS Attacks. *Cyber Physical Security and Privacy (IEEE 2011 smart GridComm)*. Pp 226-228...
  76. Jyoti Grover, Ashish Jain A, Sunita Singhal, and Angu Yadav. “Real-Time VANET Applications Using Fog Computing”. *Springer Nature Proceedings of First International Conference*, pp. 683-685.
  77. Vaibhav Eknath Narawade, and Uttam D. Kolekar. “EACSRO: Epsilon constraint-based Adaptive Cuckoo Search algorithm for Rate Optimized Congestion Avoidance and Control

- in Wireless Sensor Networks”. IEEE 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), pp 715-720.
78. Gurleen Kaur . “A preventive approach to mitigate the effect of gray hole using genetic algorithm”. 2016 IEEE International Conference on Advanced in Computing, Communication, Automation (ICACCA) .pp 1-2.
79. Fuad A. Ghaleb , Anazida Zainal Murad A. Rassam Fathey Mohammed. “An effective misbehavior detection model using artificial neural network for vehicular ad hoc network applications”. 2017 IEEE Conference on Application, Information and Network Security (AINS) pp 1-3.
80. Ruining Zhang, Xuemei Jiang, & Ruifang Li. “Decomposition based multi objective spectrum allocation algorithm for cognitive vehicular networks”. 2017 IEEE 17th International Conference on Communication Technology (ICCT). Pp. 831 – 836.
81. Karan Verma, & Halabi Hasbullah.”IP-CHOCK (filter)-Based Detection Scheme for Denial of Service (DoS) attacks in VANET”. IEEE, 2014. 2014 International Conference Computer and Information Sciences (ICCOINS). pp 1-6.
82. Abdul Quyoom, Raja Ali, Nandan Gouttam, Harish and Sharma. “A Novel Mechanism of Detection of Denial of Service Attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)”. International Conference on Computing, Communication and Automation (ICCCA2015). Pp 414-416.
83. Nikita Lyamin, Alexey Vinel, Magnus Jonsson M., and Loo J. “Real-Time Detection of Denial-of-Service Attacks in 2014 IEEE 802.11 p”. IEEE Communications Letters. Vol. 18, pp. 110-112.
84. Georgios Karagiannis, Onur Altintas, Eylem Ekici, Geert Heijenk, Boangoat Jarupan ,

- Kennet Lin, and Timothy Weil. "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions", IEEE 2011 Communications Surveys & Tutorials, 2011, Vol. 13, pp 584-590.
85. Yongxu Lai, Lu Zhang, Tian Wang, Fan Yang, & Yifa 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, July 2017, pp. 227-236.
86. Ammara Anjum Khan, Mehran Abolhasan, & Wei Ni, W. (2018). "5G next generation VANETs using SDN and fog computing framework". In Consumer Communications & Networking Conference (CCNC), 2018 15th IEEE Annual .pp. 1-6.
87. Omprakash Kaiwartya, Sunshil Kumar, D. K. Lobiya, Abdul Hanan Abdullah, and Nazer Hassan. "Performance Improvement in Geographic Routing for Vehicular *Ad Hoc* Networks". *Sensors* **2014**. Pp 22348-22351.
88. Carsten Buttner, Friederike Bartels, and Sorin Huss. "Real-World Evaluation of an Anonymous Authenticated Key Agreement Protocol for Vehicular Ad-Hoc Networks". 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). Pp 652-654.
89. Ram Shringer Raw, Sanjoy Das. "Performance analysis of P-GEDIR protocol for vehicular adhoc network in urban traffic environments". *Wireless Personal Communication* November **2013**, Vol. 68, pp. 65–78.
90. Jianjun Yang, Zongmin Fei. "Broadcasting with Prediction and Selective Forwarding in Vehicular Networks". *International Journal of. Distributed Sensor Network*. December 2013, Vol. 1, pp. 1–9.

91. Artimy. “Local Density Estimation and Dynamic Transmission-Range Assignment in Vehicular Ad Hoc Networks”. IEEE Transaction Intelligent Transportation System **2007**, Vol. 8, pp. 400–412.
92. Samuel Kofi Erskine., and Khaled M. Elleithy Secure Intelligent Vehicular Network Using Fog Computing. Electronics MPDI April 2019.pp 6-8.
93. Erik Cuevas, and Adolfo Reyna-Orta A. “A Cuckoo Search Algorithm for Multimodal Optimization”. Hindawi Publishing Corporation e Scientific World Journal Volume 2014. Pp1-5.
94. Alexey Vinel, Claudia Campoo, Jonathan Petit, and Yevgeni Koucheryavy. “Trustworthy Broadcasting in IEEE 802.11p/WAVE Vehicular Networks: Delay analysis”. IEEE Communications Letters 2011. Vol 15, pp. 1010-1011.
95. Qiwu Wu, and Qingzi Liu. “A Trusted Routing Protocol Based on Bayesian in VANET”. IEEE 2014 International Conference on Cyberspace technology (CCT). Pp 1-4.
96. Zhaolong Ning, Jin Huang, and Xiaojie Wang. “Vehicular Fog Computing: Enabling Real-Time Traffic Management for Smart Cities”. IEEE 2019 Wireless Communications • February 2019. Vol 26, pp. 87-88.
97. Khondokar Fida Hasan, Charles Wang, Yanming Feng, and Yu-Chu Tian. “Time synchronization in vehicular ad-hoc networks: A survey on theory and practice”. 2018 Vehicular Communication. ScienceDirect. School of Electrical Engineering and Computer Science, Queensland University of Technology Vol. 14, pp. 40-41.