AN EFFICIENT DDoS ATTACK DETECTION FRAMEWORK FOR VEHICULAR COMMUNICATION

RAENU A/L KOLANDAISAMY

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

2020

AN EFFICIENT DDoS ATTACK DETECTION FRAMEWORK FOR VEHICULAR COMMUNICATION

RAENU A/L KOLANDAISAMY

THESIS SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

2020

UNIVERSITY OF MALAYA
ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: Raenu Kolandaisamy

Matric No: WHA130007

Name of Degree: Doctor of Philosophy

Title of Project Paper/Research Report/Dissertation/Thesis ("this Work"): Thesis

Field of Study: Network & Security

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;
(2) This Work is original.
(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
(4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
(5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
(6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature Date: 4/5/2020

Subscribed and solemnly declared before,

Witness's Signature Date: 4/5/2020

Name:

Designation:

AN EFFICIENT DDoS ATTACK DETECTION FRAMEWORK FOR VEHICULAR COMMUNICATION

ABSTRACT

Vehicular Ad Hoc Networks (VANETs) are rapidly gaining attention due to the diversity of services that they can potentially offer. VANET is a wireless network that allows vehicles to interconnect and communicate with other nearby vehicles and Road Side Units (RSUs). In VANET, each vehicle is considered as a node which is equipped with an On-Board Unit (OBU) and an Application Unit (AU). The nodes may connect and communicate with each other directly (i.e., Vehicle to Vehicle (V2V)) or through RSUs (i.e., Vehicle to Infrastructure (V2I)). This is primarily for alleviating an Intelligent Transport System (ITS) that aims to provide a wide range of applications and services including safety, non-safety, and infotainment. The aim of this research is to enhance the detection of DDoS attacks on vehicular communication in VANET environments. This enhanced detection of DDoS attack will provide secure and safe vehicular environment for the drivers and passengers to access the VANET applications and services without having to face disturbance or unavailability of services. However, VANET communication is vulnerable to numerous security threats such as Distributed Denial of Service (DDoS) attacks. Dealing with these attacks in VANET is a challenging problem. Most of the existing DDoS detection techniques suffer from higher detection time. To overcome these problems, we present an efficient DDoS attack detection framework which consists of important techniques, i.e. MVSA and SPPA. During V2V communication, DDoS attacks may occur without the users/drivers realizing or being fully aware about it. In the MVSA model we consider small scale vehicular environments. The

MVSA model maintains the multiple stages for the detection of DDoS attacks in vehicular networks. The model observes the traffic in different situations and time frames and maintains different rules for various traffic classes in various time windows. In the SPPA model, a cluster-based attack detection in data collection was considered, where the leaf nodes pass the sensitive information to the cluster head. The existence of malicious nodes threatens decision making by sending malicious information and sometimes sending many packets to the vehicle node. To overcome this issue, a Stream Position Performance Analysis (SPPA) model has been proposed. This model is used for big scale vehicle environments. This approach monitors the position of any field station in sending the information to perform a Distributed Denial of Service (DDoS) attack. The performance of the MVSA and SPPA methods is evaluated using a Ns2 simulator. Simulation results demonstrate the effectiveness and efficiency of the MVSA and SPPA regarding attack detection time and reducing the impact on vehicular communication on VANET.

Keywords: VANET, Security, DDoS Attack, Ns2 Simulation, Safety Application

RANGKA KERJA KECEKAPAN PENGESANAN SERANGAN DDoS BAGI KOMUNIKASI KENDARAAN

ABSTRAK

Vehicular Ad Hoc Networks (VANETs) mendapat perhatian yang mendadak kerana kepelbagaian tawaran perkhidmatan. VANET adalah rangkaian tanpa wayar yang membolehkan kenderaan untuk sambung dan berkomunikasi dengan kenderaan lain yang berdekatan. Dalam VANET, setiap kenderaan dianggap sebagai nod yang dilengkapi dengan On-Board Unit (OBU) dan Application Unit (AU). Nod boleh berhubung dan berkomunikasi antara satu sama lain secara langsung (contohnya, kenderaan ke Kenderaan (V2V) atau melalui Road Side Unit (RSU) (contohnya, kenderaan untuk Infrastruktur (V2I). Ini adalah terutamanya untuk mengurangkan Sistem Pengangkutan Pintar yang bertujuan untuk menyediakan pelbagai aplikasi dan perkhidmatan termasuk keselamatan, bukan keselamatan dan infotainment. Tujuan kajian ini adalah untuk meningkatkan pengesanan serangan DDoS pada kenderaan untuk kenderaan yang berkomunikasi dalam persekitaran VANET. Dengan pengesanan pintar DDoS, ia akan menyediakan persekitaran rangkaian kenderaan selamat, selamat untuk pemandu dan penumpang untuk mengakses aplikasi dan perkhidmatan VANET tanpa menghadapi gangguan atau ketiadaan perkhidmatan. Walau bagaimanapun, VANET komunikasi adalah terdedah kepada pelbagai ancaman keselamatan seperti serangan Distributed Denial of Service (DDoS). Serangan dalam VANET ini merupakan masalah yang mencabar. Kebanyakan teknik pengesanan DDoS yang sedia ada mengalami masa pengesanan lebih tinggi. Untuk mengatasi masalah ini, model novel Multivariant Stream Analisis (MVSA) telah dibentangkan, di mana model ini digunakan untuk persekitaran kecil-kecilan. Pendekatan MVSA yang dicadangkan mengekalkan pelbagai peringkat untuk mengesan serangan DDoS di dalam kenderaan untuk kenderaan komunikasi dalam

persekitaran VANET. Dalam rangkaian VANET, nod kenderaan akan bergerak dengan pantas dari satu tempat ke tempat lain, dimana serangan DDoS akan berlaku dalam rangkaian VANET. Penyelidik akan melaksanakan pengesanan berdasarkan tahap komunikasi serangan DDoS ke atas rangkaian VANET. Nod sumber akan menghantar data ke destinasi menggunakan nod pertengahan, pada masa yang sama mana-mana serangan DDoS akan berlaku pada nod. Dalam model kedua, penyelidik mengambil kira pengesanan serangan berasaskan kelompok dalam pengumpulan data di mana nod daun memberikan maklumat sensitif kepada kepala kluster. Kewujudan nod berniat jahat mengancam pembuat keputusan dengan menghantar maklumat yang berniat jahat dan mungkin menghantar sejumlah besar paket kepada nod kenderaan. Untuk mengatasi masalah ini, penyelidik telah mencadangkan satu model Stream Position Performance Analysis (SPPA). Model ini digunakan untuk persekitaran kenderaan yang besar. Pendekatan ini memantau kedudukan mana-mana stesen bidang dalam menghantar maklumat untuk melakukan serangan DDoS. Prestasi MVSA dan kaedah SPPA dinilai dengan menggunakan simulator NS2. Dapatan simulasi menunjukkan keberkesanan dan kecekapan MVSA dan SPPA berkaitan masa pengesanan serangan dan mengurangkan kesan ke atas kenderaan untuk kenderaan komunikasi pada rangkaian VANET.

Kata Kunci: VANET, Sekuriti, Serangan DDoS, Ns2 Simulasi, Aplikasi Keselamatan

ACKNOWLEDGEMENTS

I would like to thank my first advisor, Associate Professor Dr. Rafidah Md Noor and second advisor Dr. Muhammad Reza Z'aba, for supporting me during these past 6 and half years. Dr. Rafidah Md Noor is someone you instantly love and never forget once you meet her. She is the knowledgeable advisor and one of the smartest people whom I know. I hope that I could be as lively, enthusiastic, and energetic as Dr. Rafidah Md Noor. Dr. Muhammad Reza Z'aba is someone you instantly love and never forget once you meet him. Dr. Reza help me a lot on thesis editing.

I especially thank to my parent's father M. Kolandaisamy, mother P. Sundrambal, my wife Dr. M. Thevimalur, son R. Viishnu, daughter R. Banu, sisters Ko Kavetha, K. Sharalla & K. Indraah and brother in laws. My hard-working parents have sacrificed their lives for my sisters and myself and provided unconditional love and care. I love them so much, and I would not have made it this far without them. My wife has been my best friend all my life and I love dearly and thank them for all their advices and supports.

"I dedicate this thesis to

my beloved dad, mum, wife, son, daughter and my sisters

for their constant support and unconditional love.

I love you all dearly"

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ATM	Asynchronous Transfer Mode
ACK	Acknowledge
AMS	Advanced Marking Scheme
A-NIDS	Anomaly Based Network Intrusion Detection System
AODV	Ad Hoc On-demand Distance Vector
ASP	Augmented Split-Protocol
AU	Application Unit
BS	Base Station
BSSID	Basic Service Set Identification
CBR	Constant Bit Rate
CCH	Control Channel
CH	Cluster Head
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
DR	Detection Rate
DSRC	Dedicated Short Range Communication
EAACK	Enhanced Adaptive Acknowledgement
ECC	Elliptic Curve Cryptography (ECC)
EDAODV	Early Congestion Detection & Control Routing Protocol
FCC	Federal Communications Commission
FPR	False Positive Rate

GSM	Global System for Mobile Communications
H-IDS	Hybrid Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISP	Internet Service Provider
ITS	Intelligent Transport System
JSK	Jidosha Soko Densi-gijutsu Kyokai
KDC	Key Distribution Center
LAN	Local Area Network
LPN	Local Protection Node
MANET	Mobile Ad-hoc Network
MP	Matching Pursuit
MVND	Malicious Node Detection Algorithm
MVSA	Multi Variant Stream Analysis
NID	Network Intrusion Detection
NIPS	Network Intrusion Protection System
Ns2	Network Simulation Version 2
OBU	On Board Unit
ODR	Overall Detection Rate
ODR	Overall Detection Rate
OMP	Orthogonal Matching Pursuit
PDR	Packet Delivery Ratio
PIDAD	Packet Identification Anomaly Detection
PSOBU	Public Safety On-Board Unit

QoS	Quality of Service
R&D	Research and Development
RBF	Radial Basis Function
RO	Routing Overhead
RPN	Remote Protection Node
RSU	Road Side Unit
RTI	Road Transport Informative
SINR	Signal-to-Interference-Plus-Noise Ratio
SPPA	Stream Position Performance Analysis
SUMO	Simulation of Urban Mobility
SYN	Synchronizes
TCP	Transmission Control Protocol
UMTS	Universal Mobile Telecommunications System
UWB	Ultra-Wideband
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VANET	Vehicular Ad-hoc Network
VoIP	Voice over IP
WAVE	Wireless Access in Vehicular Environment
WCMP	Wireless Short Message Protocol
Wi-Fi	Wireless Fidelity
Wi-MAX	Worldwide Interoperability for Microwave Access
WSN	Wireless Sensor Network
WWW	World Wide Web

CHAPTER 1: INTRODUCTION

1.1 Introduction

Vehicular Ad-hoc Network (VANET), a subclass of the Mobile Ad-Hoc Network (MANET), is a wireless network that can help a vehicle to communicate with other nearby vehicles and roadside infrastructure. It appears as one of the latest technologies to improve the new generation of wireless networking to vehicles. With the increase in the number of cars, there is a higher demand for inter-vehicle communication. As technology advances, VANET is gaining significant attention in the automotive industry due to safety concerns in transportation. The architecture and components of VANET are depicted in Figure 1.1.

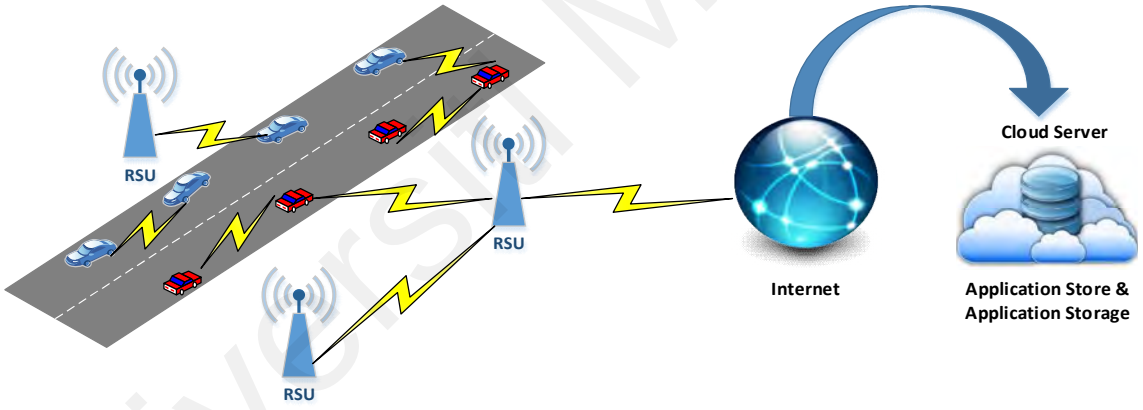

Figure 1.1: Vehicular Ad-hoc Network Architecture

The growth of population and the need for people to use transportation to accomplish tasks is increasing. Around the world, hundreds of millions of people use road vehicles as a means of transportation. In modern society, mobility is a supreme achievement. However, the number of vehicles on the road has increased alongside greater density in traffic, incidences of collision, and road congestion. Research shows that in Europe there were 1.3 million vehicle accidents, involving 1.7 million injuries and 40,000 deaths per year (Razvodovsky, 2016), (Shield & Rehm 2015) and (Mershad & Artail, 2012). An estimated total of 160

billion euros has been allocated for direct and indirect costs (Shield & Rehm 2015). The rest of the world is also faced with the same problem. The same research shows that almost 24% of our driving time is spent in traffic jams (Shield & Rehm 2015). VANET has been known to accomplish a safer driving environment through intelligent and computerized vehicles, technology-equipped roads, high mobility and rapid changes in network topology (Elsadig & Fadlalla, 2016). VANET is one of these communication networks but it is used for communicating between the vehicles and nearby base stations.

There are two main communications models and patterns in VANET which can be classified into Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. V2V involves sending or sharing information between vehicles in the VANET. V2V only allows communication among vehicles such as alerting and notifying drivers but does not involve taking control of the vehicle when there is an emergency (DaCunha et al., 2014). V2I will send info to other vehicles via RSU. RSU will forward the info to the other vehicles. Jidosha Soko Densi-gijutsu Kyokai (1980) proposed the idea of V2V. Besides that, California PATH (Partners for Advanced Transit and Highways) and Chauffeur of the EU (Europe) have also shown the technique of combining 2 or more vehicles together electronically so that to create a train. Europe also has a few large-scale programs which are now in progress under the Road Transport Informative (RTI). It is equivalent to the US Intelligent Transport System (ITS).

The communication technology developed so far is used mainly for stabilizing ITS in road traffic. VANET consists of three main types of unit: Road Side Units (RSU), On-Board Units (OBU) and Application Units (AU). RSUs are normally installed along the road side to provide information exchange support with vehicles. They act like relays to further extend

the network coverage. OBUs are installed in vehicles to allow periodic exchange of information with other vehicles for a safer and more comfortable driving experience. There is a specific type of OBU, the Public Safety On-Board Unit, which gives certain traffic signal priority to safety vehicles like ambulances, police cars or fire trucks. Last, the function of the AU is to execute the programme to enable the OBU to communicate with other nodes or RSUs.

One of the important safety aspects in VANET is security. To be fully functional, the network must be available always because during an emergency a node needs to send information to other nodes. Due to the nature of ad hoc technology and the way it operates, VANET is faced with several security threats. To provide a safe and efficient traffic environment, the exchange of timely traffic information between vehicles is important so that the driver can analyze the traffic environment early. This can be achieved by developing the ITS (Sahare & Malik, 2014). ITS as a useful application implemented by the VANET and provides several services to help in traffic management. Besides that, ITS can solve major issues in traffic management such as traffic jams, or driver or passenger safety by integrating traffic information and communication technologies into transportation infrastructure and vehicles.

The vehicles and RSUs act as both transmitters and receivers. The mobility of vehicles is continuous and very fast, especially on highways. Thus, the communication links between vehicles are established only for a short period of time; that is, vehicles are rapidly connecting and disconnecting in the network. This is due to the quickly changing topology. However, the mobility of vehicles is predictable as they move on prebuilt highways and roads. Hence the motion pattern of the vehicles can be predicted based on road topology and

layout. The nodes in a VANET move at a higher average speed compared to MANET. The number of nodes in a VANET can be very high on busy highways and very sparse in remote highways. Similarly, at a particular location, traffic is at its busiest during office hours and is quiet during midnight hours. Hence, any protocol designed should take into consideration these scenarios. Each vehicular node may acquire a service through various RSUs, or the packets might have to travel through several nodes, which makes the network vulnerable to Denial of Service (DoS) attacks.

In VANET, DoS attacks (Sinha & Mishra, 2013) attempt to disrupt the communication channel by flooding it with redundant messages so that legitimate nodes can no longer acquire services. A Distributed Denial of Service (DDoS) attack (Sahare & Malik, 2014) is more severe, as the attack is larger in scale. It involves the participation of multiple nodes across the Internet that the attacker maliciously controls. In a DDoS attack, the attacker may overwhelm the network by using different time slots to send the messages or changing all time slots and messages for different nodes. It is imperative to prevent these types of attacks from crippling the network and to allow it to continue its services for safety applications. There are two possible scenarios that can happen when a DDoS attack is launched. Figure 1.2 illustrates DDoS in V2V communications and Figure 1.3 illustrates DDoS in V2I communications.

a) **Vehicle-to-Vehicle (V2V)**: Attackers send beacon messages to a victim from different locations or vehicles with the possibility of using different time slots. This attack is intended to control/collapse the network and because of this, life critical information will be unavailable to the victim (Sinha & Mishra, 2013). The other causes of this attack are service unavailability, floods of messages from the attacker, bottlenecks and bandwidth starvation.

After the attack successfully breaks down the network, the network service will no longer exist because the network node will not be able to send and receive messages. Transmitting incorrect information among vehicles will potentially lead a vehicle driver to make wrong decisions during driving. This is because a normal driver cannot recognize network attacks.

b) **Vehicle-to-Infrastructure (V2I)**: Instead of targeting vehicles, the attacker targets the RSUs. The attack will come from different locations and if there are other nodes that want to communicate with the RSU, it has already been overloaded. Hence, the service is not available (Sinha & Mishra, 2013).

To establish a VANET, the 802.11p network standard is used. This is because 802.11p can provide lower latency of short-range communication. Dedicated Short Range Communication (DSRC) with 75MHz of spectrum in the 5.9GHz band is allocated in the United States and used in ITS. In Europe, a DSRC with 30 M Hz of spectrum in the 5.9Hz band is used (Li, 2010) (Morgan, 2010). Europe also has a few large-scale programs which are under the Road Transport Initiative (RTI).

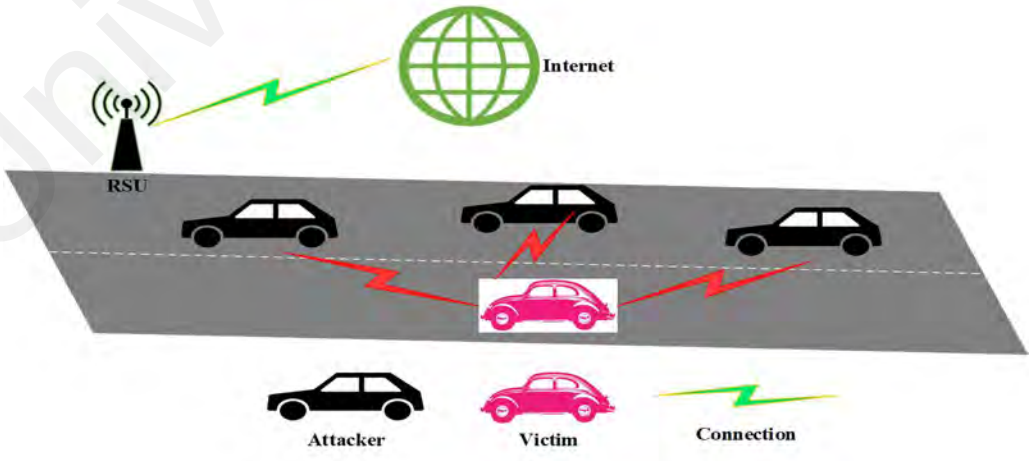

Figure 1.2: DDoS in Vehicle to Vehicle Communications

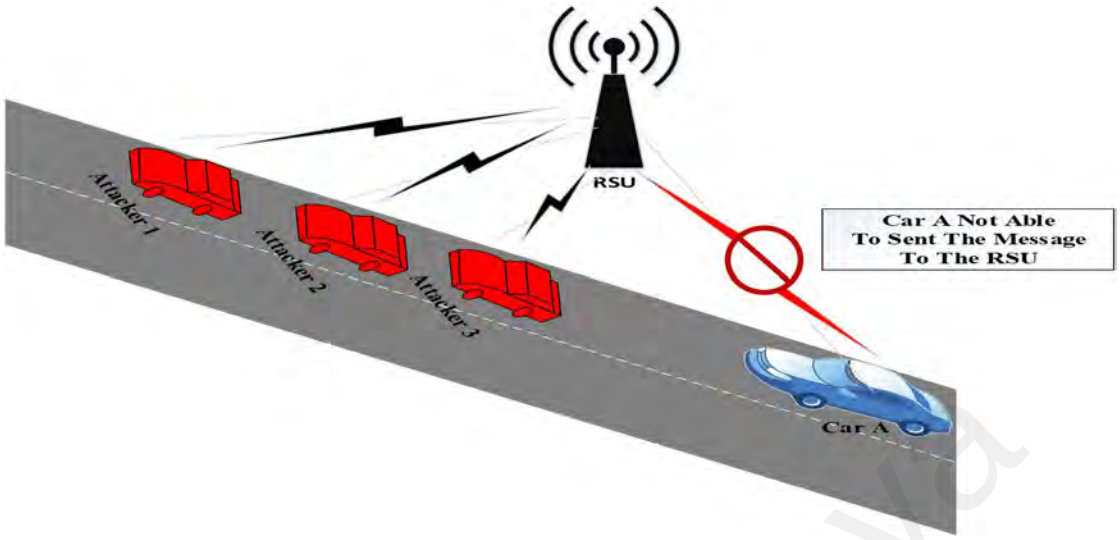

Figure 1.3: DDoS in Vehicle to Infrastructure Communications

Although VANET has its own distinct characteristics compared to other networks, there still exist various challenges with VANET especially in security (Chaubey, 2016). Recently, VANET faced many security threats that may cause service abuses or service degradation (Azees, Vijayakumar & Deborah (2016), Bariah, Shehada, Salahat & Yeun (2015) and Elsadig & Fadlalla (2016)). Due to this issue, the traffic management in ITS will be affected, and the traffic environment will become dangerous. Therefore, security in VANET should not be neglected in the traffic environment.

1.1 Problem Statement

A DDoS attack is considered one of the most severe attack in VANET. The attack causes huge problems to drivers on the road since vehicles are unable to exchange vital real-time information due to the unavailability of the service. It may also lead to car accidents (Razvodovsky, 2016). Defending against DDoS attacks is not easy. In some cases, DDoS attacks have been used as a distraction to divert attention while the attackers attempt to gain access to the network by using other methods that are unnoticeable while the DDoS attack

is progressing (Kaur & Sandhu (2016), (Navaz, Sangeetha & Prabhadevi (2013), Ayonija & Jain (2013)). This is one of the main reasons why this research focuses on DDoS attacks.

Moreover, VANET has a highly dynamic topology, i.e. nodes are constantly leaving and joining the network. Therefore, authentication and verification of the nodes are highly important to allow us to recognize nodes that entered the network. Many related works (Bansal, Sharma & Prakash (2015), Biasi, Vieira & Loureiro (2018), VIPIN & Chhillar (2018), Shabbir, Khan & Saqib (2016), Sahare & Malik (2014) and Pathre, Agrawal & Jain (2013)) have proposed VANET attack detection mechanisms but they did not identify or classify the packets according to their importance before they are blocked/dropped. In addition, previous methods did not store histories of attacks to identify genuine attackers. The attack history is important since, if the same attack pattern is detected in the VANET network, then the corresponding packets will be quickly identified and eliminated from the network. There are still limitations inherent in existing methods in terms of throughput, end to end delay, packet delivery ratio, attack detection rate, attack detection time and false classification ratio. All the current methods take more time to detect a DDoS attack. An attack detection rate indicates the proportion of how often the system successfully detects a DDoS attack from start to finish, and the percentage of nodes are correctly identified by the system to be falling under attack.

An efficient DDoS attack detection method would provide a secure and safe vehicular networking environment for road users. This is to ensure that the drivers and other road users can gain access to the VANET safety applications and the network 24 hours a day and 7 days a week, at any time or any location without experiencing any disturbance to the VANET

services. This is also to ensure that every driver and passenger can travel safely on every trip and avoid road accidents.

1.2 Research Motivation

The motivation for this research is to enhance the detection of DDoS attacks in VANET environments. This will provide a more secure and safe vehicular network environment for drivers and passengers to access the VANET applications and services without having to face disturbance to or unavailability of services. Unfortunately, there are many irresponsible people who disturb the VANET network by attacking it. The current detection methods suffer from high computational overhead (processing time) and it takes some time to detect a DDoS attack (Bansal, Sharma & Prakash (2015), (Biasi, Vieira & Loureiro (2018), VIPIN & Chhillar (2018), Shabbir, Khan & Saqib (2016), Sahare & Malik (2014), Pathre, Agrawal & Jain (2013)). In road safety and other time-critical applications, the network has strict delay constraints. It is very crucial that the messages communicated via the VANET reach the participating nodes on time. The main motivation of this research is to improve the detection of a DDoS attack during vehicular communication at its early stage.

1.3 Research Aim

The aim of this research is to enhance the detection of DDoS attacks in VANET environments. This enhanced detection of DDoS will provide a secure and safe vehicular network environment for the drivers and passengers to access VANET applications and services without having to face disturbance or unavailability of services.

1.4 Research Objectives

1. To analyze the characteristics of DDoS Attacks in VANET.
2. To design a framework for detecting a DDoS attack in the vehicular environment:
    2.1 Multi Variant Stream Analysis (MVSA)
    2.2 Stream Position Performance Analysis (SPPA)
3. To evaluate the framework using a Network Simulator and benchmark the proposed framework based on existing models.
4. To validate the proposed framework using statistical tools.

1.6 Research Contributions

The study is valuable for VANET users as it offers a new set of concepts, specifically in the area of security. VANET has provided the wireless communication network in order to manage the road traffic. By implementing the VANET in the ITS, every vehicle can communicate with each other through the RSU and OBU. The researcher has proposed a framework to detect DDoS attacks in VANET environments. The first framework is MVSA, and the second framework is SPPA. At the end of the process, attacks have been classified, and neighbours can be informed about the DDoS attack. In the future, if the same patterns of packets enter the RSU, then the RSU will discard the packets.

1.7 Research Benefit

The study is valuable for VANET users as it offers a new perspective on network security in VANET environments. Furthermore, the main reason for this researcher to choose the topic is that the VANET technology can decrease the number of road crashes and the percentage of deaths on the roads. Also, one important outcome of this work is that it will provide some useful information about VANET to the people of Malaysia. Certainly, this study has a

number of major implications for the policy makers, practitioners and academics in the constantly changing road safety situation in Malaysia.

1.8 Chapter Organization

Chapter 1: This chapter in particular will give a basic introduction to VANET, a background to DDoS attacks, as well as the research problems and the objectives of this study. Apart from that, the contribution made by this study will also be explained.

Chapter 2: This chapter will discuss the state-of-the-art in VANET. Besides that, the literature review on DoS Attacks, DDoS attacks, VANET Classification and safety and non-safety applications will be discussed in this chapter.

Chapter 3: This chapter will carry out the deep problem analysis on DDoS attacks in vehicular communication. Besides that, some history of DoS and DDoS attacks are given. Finally, some statistics on DDoS attack detection methods are discussed.

Chapter 4: This chapter discusses and analyses the design of Multi Variant Stream Analysis and Stream Position Performance Analysis frameworks for VANET services. It focuses more on methods, attacks and application classsification.

Chapter 5: This chapter will focus on simulation. Test results for DDoS attacks, VANET classes and experimental results will be explained thoroughly in this chapter. Besides that, the validation framework will be discussed. In addition, the SPPA framework results will be validated using Mini-Tab version 18.

Chapter 6: This chapter will conclude this research work. In addition, some recommendations will be provided. The future directions of research arising from this study will also be justified.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This chapter provides an in-depth review of VANET, its characteristics and challenges. Nevertheless, safety applications, non-safety applications and infotainment applications were are also discussed in the context of VANET. This Review, then, is organized as follows. Section 2.2 provides an overview of the architecture of VANET, Section 2.3 discusses Intelligent Transportation Systems, Section 2.4 covers components of VANET, and Section 2.5 will discuss communication in VANET. Next, Section 2.6 & Section 2.7 will comment on VANET's characteristics and challenges. In Section 2.8, VANET applications are covered, followed by security mechanisms in VANET in Section 2.9. Sections 2.10 and 2.11 discuss the taxonomy of attackers and attacks in VANET. Finally, in Section 2.12 various detection approaches are discussed.

2.2 Architecture of VANET

VANET stands for Vehicular Ad-Hoc Networks and is an autonomous system with a large collection of vehicular nodes that can move freely but with some restrictions. VANET was created in October 2002 by the Federal Communications Commission (FCC) (Cunha et al., 2014). The aim of its creation was to improve road safety. VANET is a form of Mobile Ad Hoc Network and it became an important component of Intelligent Transportation Systems (ITS). VANET facilitates users to communicate with each other without any physical infrastructure (Zeadally et al., 2012). In spite of any geographical location, it keeps the network to connect dynamically, thus forming an infrastructure with less network of its own. It has been utilized in wireless communications, where each node contributes as a source, destination and intermediate router.

The Vehicular nodes are smaller, cheaper and more powerful with applications and network services to run, which makes the VANET a rapidly growing technology. Each node in VANET can communicate with nodes within its transmission range directly, but nodes beyond the range perform multiple hops to relay the packets. Therefore, the node should dynamically discover its own route (Zeadally et al., 2012). Any node has the capability to join or leave the network at any time and it performs a cooperative transmission of packets by transmitting and receiving from another node. There is no special router for the transmission and reception of packets. Here the node performs both as a host and a router by taking its own decision to perform routing for forwarding the packet.

Basically, VANET technology is used to enhance a safe and effective traffic environment by allowing communication between vehicles. In other words, VANET is an infrastructure-less network and it is built-on self-organizing. Besides that, there are two types of communication in VANET which are Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I). To create a VANET environment, there are three important components that cannot be neglected which are Road Side Units (RSU), Application Units (AU) as well as On Board Units (OBU) (Hasrouny et al., 2017). In detail, every node in a VANET environment has been attached to the OBU and AU. OBUs are the radio devices which can carry out communication within VANET environments, while the function of the AU is to execute the software to make the OBUs communicate (Hasrouny et al., 2017). Moreover, RSUs are installed along the road side and are connected to other vehicles, Internet and base stations. Figure 2.1 shows the Vehicular Ad-hoc Network Scenario and Figure 2.2 shows the VANET Architecture. In VANET, there were two main communications models, namely Vehicle-to-Vehicle Communication (V2V) and Vehicle-to-Infrastructure Communication (V2I).

a) Vehicle-to-Vehicle Communication (V2V)

The communication between vehicles. Vehicles used to communicate and send messages/information to and from each other without any help from infrastructure. In the V2V communication, the vehicles will alert, update and notify the drivers about the condition of the road and the weather. But it does not take control of the car when there is an emergency (Yaqoob, 2017).

b) Vehicle-to-Infrastructure Communication (V2I)

The V2I is almost the same as V2V, but instead of sharing information with other vehicles, the information shared by vehicles will go to the RSU. The information can also be sent and delivered to the other vehicles via the RSU. In some places traffic will be lower or non-existent, so here, vehicles will send the updates, share important messages or request information from the RSU (Yaqoob, 2017) (Li & Lee, 2005).

Shield & Rehm (2015) and Razvodovsky (2016) shows that there were 1.3 million accidents, 1.7 million injuries and 40,000 deaths in a year. 160 billion euros has been estimated to cover direct and indirect costs. The same research showed that almost 24% of driving time is spent in traffic jams. As we know the VANET is a novel class of MANET or wireless networks which are naturally created among moving vehicles outfitted with wireless boundaries that may possibly be of identical or heterogeneous technologies. The VANETs, are believed as ad hoc networks with realistic or real-life applications allowing interaction between immediate vehicles as well as among vehicles and neighboring permanent equipment, generally defined as RSU equipment (Ahmad et al., 2016). Vehicles most of the time can be also private, belonging to personal or public transportation or private firms, (e.g., public

service vehicles such as fire engines or police cars and buses). Secure equipment can fit in to the private network or government operators or service providers.

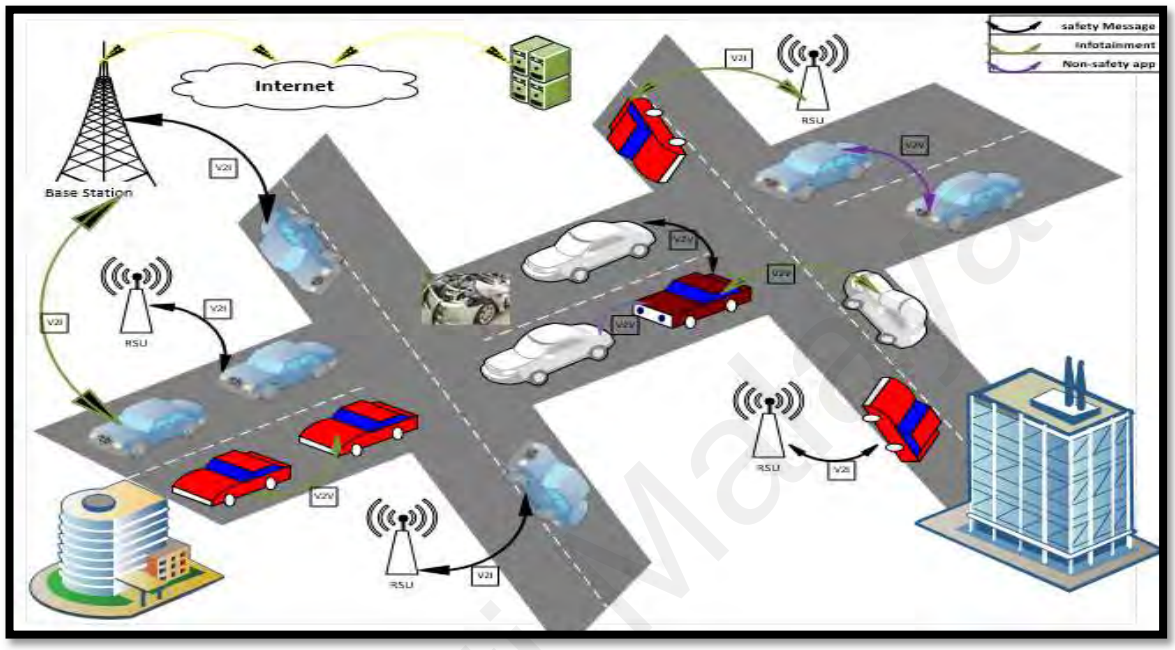

Figure 2.1: Vehicular Ad-hoc Network Scenario

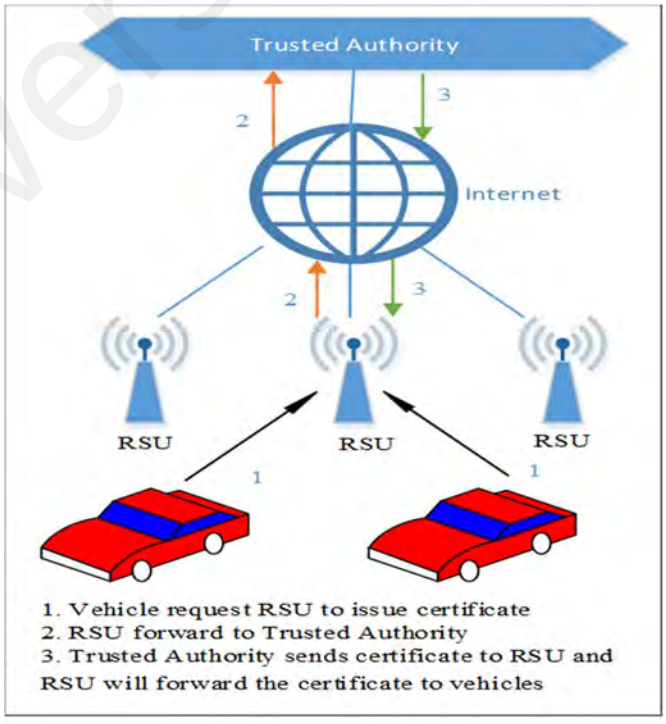

Figure 2.2: VANET Architecture

VANET is an entirely mobile network whose connections comprise of cars or vehicle outfitted together with a human machine interface and wireless routers that functions as a head-up show for alerts and as a flash monitor for infotainment or business services. Additionally, VANETs comprise of wireless outfitted RSUs that offer drivers with info regarding their instant region and can offer interaction with other communications, such as the Internet. RSUs can be any qualified packet pass on equipment such as towers or GSM. These RSU are further helpful when a single driver is separated from another VANETs since the driver will however be capable to obtain the crucial information or news so long as they are inside reach of the RSU. The major purpose of these networks remains to extend enhance road safety by offering real-time warnings to motorists regarding hazards in their anticipated path and their current area (Zeadally et al., 2012). This is feasible across intercommunication with other cars and RSUs by transferring safety info. For examples comprise blind spot warning, curve speed warning and lane merge warning.

2.3 Intelligent Transportation System (ITS)

Intelligent Transport System (ITS) is a software application which is designed to manage the traffic on the roads (Zeadally et al., 2012). Figure 2.3 shows the ITS design. The main aim of ITS is to facilitate a national model transportation system which is connected to intelligent vehicles and certain infrastructure (Sinha, & Mishra, 2013). The vehicular network can be deployed by network operators and service providers or through integration between operators, providers, and a governmental authority. Recent advances in wireless technologies and the current trends in ad hoc network scenarios allow a number of deployment architectures for vehicular networks in highway, rural, and city environments. Using this technology enhances mobility, safety and environmental performance (Sahare, & Malik, 2014). ITS can only cover limited areas by installing the specific infrastructure. All vehicles

are the nodes in the ITS so users can manage the traffic easily by observing the nodes on the traffic network. ITS helps to improve decision making in real time.

In addition, ITS also has a powerful feature which is that it offers integration of data together to make a complete and good information structure environment. This kind of environment will help in traffic planning, control and management as well as boosting the effectiveness of the ITS. A common scenario for ITS applications includes collecting data using some type of sensors and then distributing the data among the communicating nodes/entities. The resulting decision is based on specific algorithms that lead to meaningful information for drivers. Many applications of ITS exist, including vehicular traffic congestion avoidance, travel time reduction, vehicular traffic density estimation, and energy-saving. To apply ITS in the traffic network, some technologies and techniques are necessary (Engoulou et al., 2014), for example, microwave, Internet, Bluetooth, GPS, geographical location, camera systems, in-vehicle systems and other equipment.

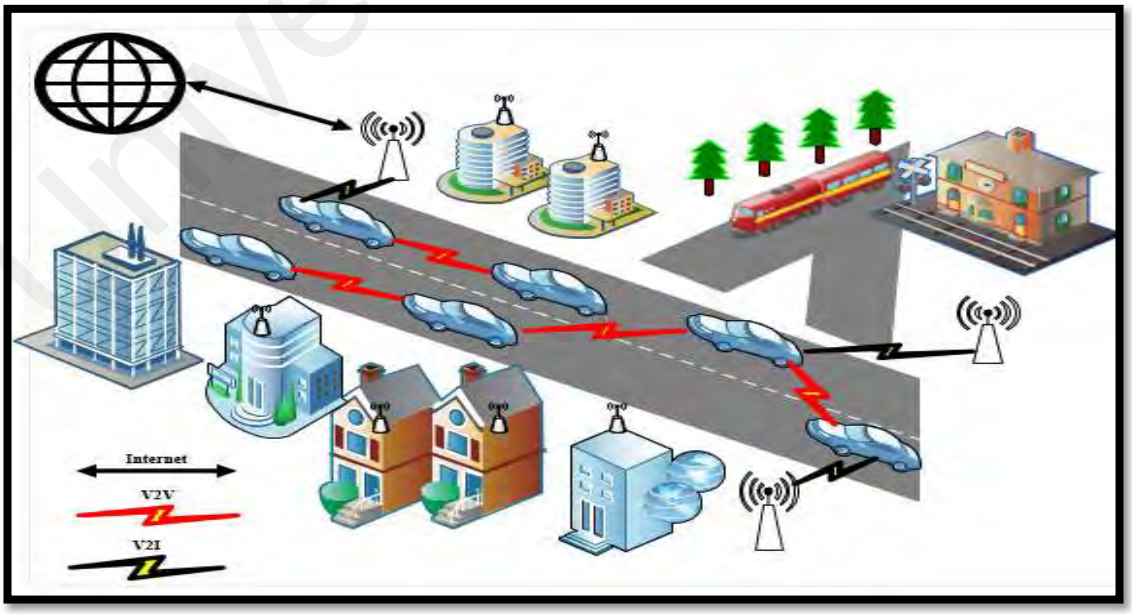

Figure 2.3: Intelligent Transportation System (ITS)

2.3.1 Vehicle-to-Vehicle Communication

The V2V communication uses multi-hop multicast/broadcast to transmit traffic related information over multiple hops to a group of receivers. In intelligent transportation systems, vehicles need only be concerned with activity on the road ahead and not behind (an example of this would be for emergency message dissemination about an imminent collision or dynamic route scheduling). There are two types of message forwarding in V2V: naïve broadcasting and intelligent broadcasting (Mejri et al., 2014), (Hasrouny et al., 2017). In naïve broadcasting, vehicles send broadcast messages periodically and at regular intervals. Upon receipt of the message, the vehicle ignores the message if it has come from a vehicle behind it. If the message comes from a vehicle in front, the receiving vehicle sends its own broadcast message to vehicles behind it. This ensures that all enabled vehicles moving in the forward direction get all broadcast messages. Figure 2.4 shows a V2V communication overview.

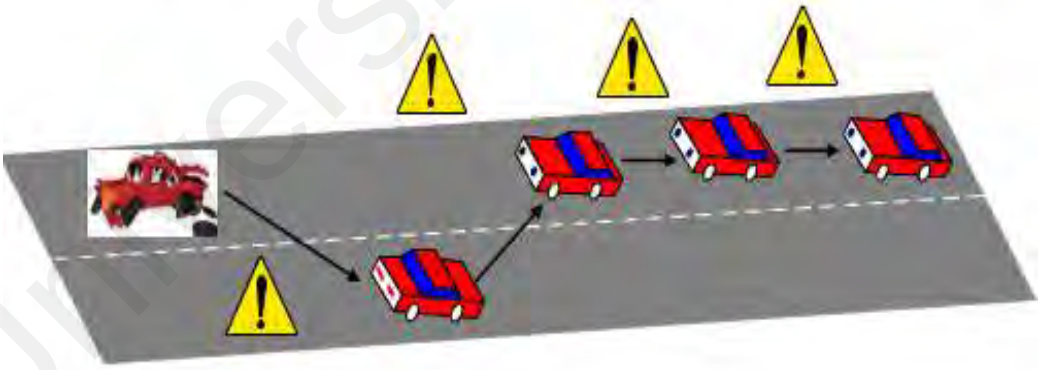

Figure 2.4: V2V Communication

The limitations of the naïve broadcasting method (Zeadally et al., 2012), (Xu et al., 2006) are that huge amounts of broadcast communications are created, consequently, expanding the probability of communication collision subsequent in reduce message transfer rates and increased delivery times. Intelligent broadcasting with implied response addresses the challenges essential in naïve broadcasting by restricting the amount of messages broadcast

for a provided alternative event. If the incident-detecting vehicle gets the similar message from behind, it believes that at minimum one vehicle in the backside has gotten it and stops broadcasting. The idea is that the vehicle in the back force be liable for shifting the message near to the remainder of the vehicles. If a vehicle gets a message from higher than one source it will perform on the initial message only.

2.3.2 Vehicle-To-Infrastructure Communication

V2I communication represents a single hop broadcast where the RSU sends a broadcast message to all equipped vehicles in the vicinity (Zhang et al., 2010), (Jafari et al., 2012). V2I communication provides a high bandwidth link between vehicles and RSU. The RSU may be placed every kilometer or less, enabling higher data rates to be maintained in heavy traffic. For instance, when broadcasting dynamic speed limits, the RSU will determine the appropriate speed limit according to its internal timetable and traffic conditions. The RSU will periodically broadcast a message containing the speed limit and will compare any geographic or directional limits with vehicle data to determine if a speed limit warning applies to any of the vehicles in the vicinity. If a vehicle violates the desired speed limit, a broadcast will be delivered to the vehicle in the form of an auditory or visual warning, requesting that the driver reduces his/her speed. Figure 2.5 shows a V2I communication overview.

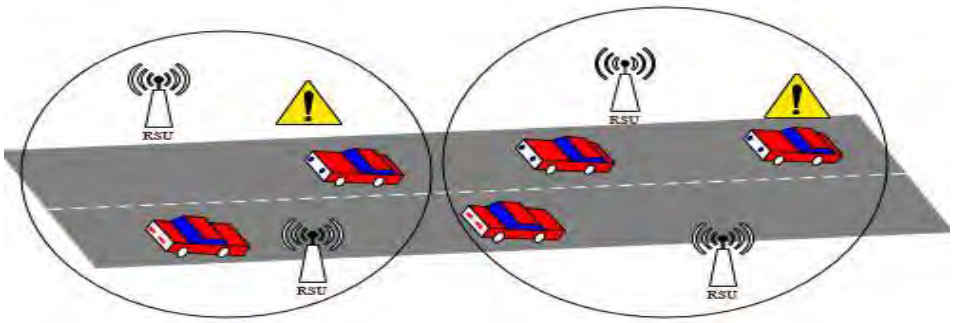

Figure 2.5: V2I Communication

2.3.3 Routing-Based Communication

Routing-based communication is a multi-hop unicast where a message is propagated in a multi- hop fashion until the vehicle carrying the desired data is reached (Pathan, 2016). When the query is received by a vehicle holding the desired piece of information, the application in that vehicle immediately sends a unicast message containing the information to the vehicle it received the request from, which is then charged with the task of forwarding it towards the query source. Figure 2.6 gives an overview of routing-based communication (Xiang et al., 2013).

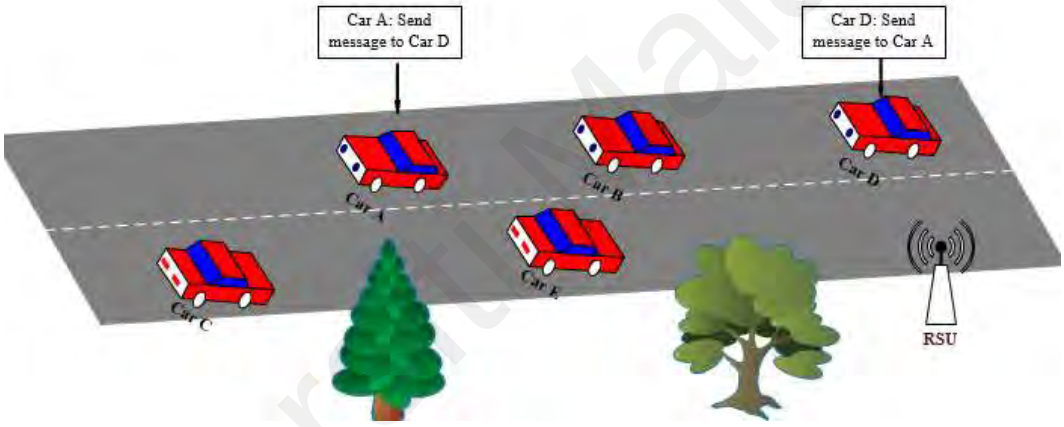

Figure 2.6: Routing-Based Communication

2.4 Components of VANET

Vehicles can communicate with the infrastructure either in a single hop or multi-hop fashion according to the vehicle's position with respect to the point of attachment with the infrastructure (Tanuja et al., 2015), (Li et al., 2015). VANET is logically composed of three types of unit, the On Board Unit (OBU), the Application Unit (AU) and the Road Side Unit (RSU). The OBU is normally used for exchanging information between RSUs and other OBUs. Figure 2.7 shows the components of the OBU. The OBU is also known as a wave device. The Recourse Command Processor (RCP) comprises OBUs that contain information.

The read and write memory is used to recover and store information. The interface of OBU is connected with short range wireless communication based on the Institute of Electrical and Electronic Engineering (IEEE) 802.11p radio technology standard (Barskar & Chawla, 2015), (Wang & Gombault, 2008). The connection between OBU and RSU will use the IEEE 802.11p radio frequency channel. In VANET network communication, the AU will send and forward messages on behalf of the OBU. Essentially, an OBU has a memory storage, is equipped with wireless communication, GPS system, easy handoff, infotainment, multiple sensors and an interactive interface for users (Yaqoob, 2017).

The AU can work within the vehicle. The vehicle uses the application provided by the service provider for communication within the OBU. The AU provides a dedicated device for safety applications and non-safety applications. Wired and wireless connections are used to connect the AU with the OBU. Most of the time the AU will reside in the OBU in a single physical unit. In most cases the OBU is dealing with all the networking functions and mobility. However, the AU will deal with the network only (Chadha, 2015), (Kumar et al., 2013).

Finally, the RSU is a computerized device or equipment that supports the connectivity and allows information sharing with the nearby passing vehicles. The main intention of the RSU is to boost the communication among vehicles and RSUs by sharing and transmitting data. It registers and authenticates the vehicles in range using tokens with unique ID as a security measure against malicious attacks. The main functions of the RSU are extending the communication range, providing internet connectivity to OBUs and providing safety applications (Sinha & Mishra, 2013), (Sahare & Malik, 2014). This may help in preventing traffic jams and accidents. RSUs will guide and assist drivers when they are going to change lanes and estimate the distance and travel time. However, RSU can provide other services

acting in different roles such as traffic directories, location servers, service proxies and more. RSU may be connected to a server to support multiple OBUs connections through internet (Engoulou et al., 2014). It is the responsibility of RSU to make the network available all the time to every node for secure communication of critical information (Singh & Sharma, 2015). For this, network availability is the major security requirement, which may be exposed to several threats or attacks. The vehicles and the RSU are prone to several security attacks such as masquerading, Sybil attacks, alteration attacks, Selfish driver attacks, etc. Among these, the Denial of Service attack is the major threat to the availability of a network. In order to shelter the VANET from DoS attacks using an enhanced attacked packet detection algorithm which prohibits the deterioration of the network performance even under this attack. The actual design of RSU is shown in Figure 2.8.

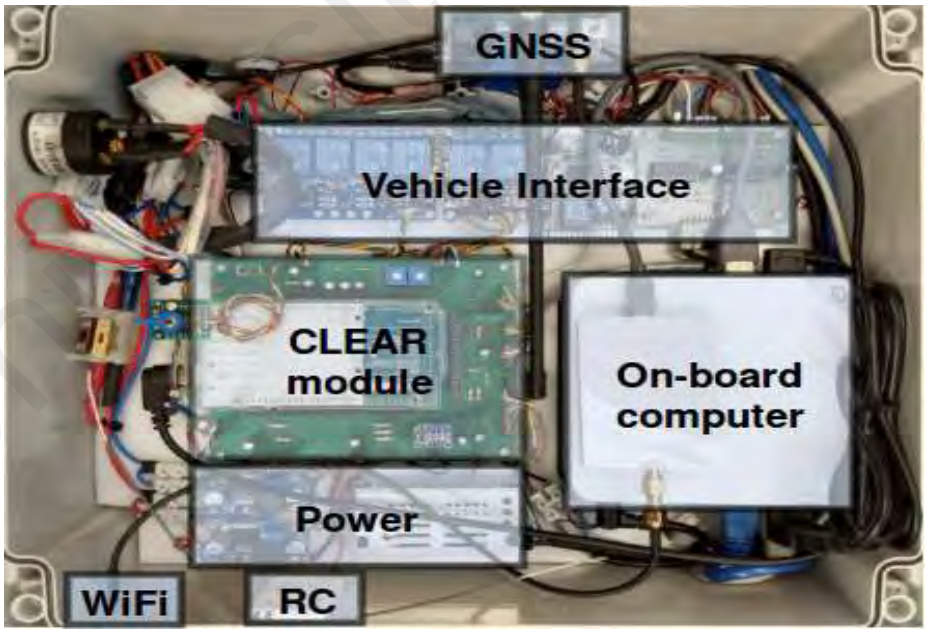

Figure 2.7: Components of On-Board Units

Figure 2.8: Road Side Unit

2.5 Communication in VANET

The concept of wireless communications in vehicles has fascinated researchers since 1980s. In the last few years, we have witnessed a large increase in research and development in this area. Several factors have led to this development, including the wide adoption (and subsequent drop in cost) of IEEE 802.11 technologies, the embrace by vehicle manufacturers of information technology to address the safety, environmental, and comfort issues of their vehicles and the commitment of large national and regional governments to allocate wireless spectrum for vehicular wireless communication (Liu et al., 2013), (Kenney, 2011). Although cellular networks enable convenient voice communication and simple infotainment services to drivers and passengers, they are not well-suited for certain direct V2V or V2I communications. However, VANETs which offer direct communication between vehicles and RSUs can send and receive warning or alert messages.

Communication in VANET is wireless based. For long range communications, Cellular Technology such as GSM based on IEEE 802.11 and Wi-Max based on IEEE 802.16 are

used. For medium range communications, 5.9 GHz DSRC standards, WAVE based on IEEE 802.11p and Wi-Fi based on IEEE 802.11g are used. Furthermore, for short range communications, Bluetooth, Zigbee, infrared and Ultra-Wideband (UWB) are used (La & Cavalli, 2014), (Barskar & Chawla, 2015), (Wang & Gombault, 2008), (Bansal, Sharma & Prakash, 2015). The specifications of DSCR and technology comparison are shown in Table 2.1.

2.5.1 Dedicated Short-Range Communication (DSRC) Channels

Dedicated Short Range Communication or DSRC is a type of technology that supports V2V and V2I communication effectively. DSRC will increase the overall efficiency and safety of the communication system. The first DSRC only has a transmission rate of 0.5Mb/s at 915MHz which is only limited for toll collection. However, with the 5.9GHz DSRC, vehicles can communicate with one another as well as the RSU and other infrastructure. Both DSRC and VANET applications will improve the overall safety of drivers on the road. The 5.9GHz DSRC enables the vehicles to receive the latest traffic information in real time regarding the surrounding environment where the vehicles are currently situated. The 5.9GHz can be accessed by any user without any usage fee since it is low in cost and easily scalable (Rasheed et al., 2017), (Vaibhav et al., 2017).

The 5.9GHz DSRC has also solved many issues that cannot be tackled by the 915MHz version DSRC. Compared with the 915MHz DSRC, obviously the bandwidth is increased. Besides, the 5.9GHz DSRC is made up of 7 channels where each channel is 10MHz while the 915MHz DSRC only supports one or maybe two channels. The transfer rate has also improved from the 0.5Mb/s of 915MHz DSRC to an interval of 6Mb/s to 27Mb/s for the 5.9GHz DSRC. In some cases, the transfer rate of 5.9GHz DSRC can reach 54Mb/s when a

20MHz channel is formed by combining two channels into one (Alam et al., 2014) and (Sudheera et al., 2016).

Table 2.1: Technology Comparison & Specification of DSRC 802.11p

Technology	Primary Use	Frequency Band	Data Rate	Range	Standard
Wi-Fi	Fixed Broadband	5 GHz	54 Mbps	35-120 Meter	802.11a
		2.4 GHz	11 Mbps	38-140 Meter	802.11b
		2.4 GHz	54 Mbps	38-140 Meter	802.11g
		2.4 GHz/5 GHz	300 Mbps	70 Meter	802.11n
	Wireless Network	5 GHz	7 Gbits	50 Meter	802.11ac
		60 GHz	7 Gbits	10 Meters	802.11ad
Wi-Max	Mobile Internet	<6 GHz	15 Mbps	1 – 3 Miles	802.16e
		6 GHz	100 Mbit/s	1 – 3 Miles	802.16M
Zig-Bee	Wireless Personal Area Network	2.4 GHz	250 Kbps	150 Meter	802.15.4
UMTS	Cellular Technology	2 GHz – 8 GHz	100 Mbps	10 – 15 Miles (its depend on tower)	4G
DSRC	V2V, V2I	5.9 GHz	6 Mbps	1000 meters	802.11p

As mentioned, there are 7 channels in the 5.9GHz DSRC, and these channels supported different types of application as shown below (Kukshya & Krishnan, 2006). The safety and non-safety channels are shown in Table 2.2.

Table 2.2: Types of Safety and Non-Safety Channels

Channels	Types	Description
Safety Channels	Channel 172	For medium power safety applications.
	Channel 178	A control channel supporting all power levels and all safety applications including announcements and V2V broadcast messages.
	Channel 184	A high-power service channel to coordinate intersection applications.

Non-Safety Channels	Channel 174	For medium power applications shared by all.
	Channel 176	For medium power applications shared by all.
	Channel 180	For low power configurations and provides slight interference when separated by 50ft and above.
	Channel 182	For low power configuration and provides slight interference when separated by 50ft and above.

Other than that, there are Channels 175 and 181 which are a combination of 2 channels. Channel 175 is a combination of Channels 174 and 176, while Channel 181 is a combination of Channels 180 and 182. Only one channel can be listened to at a time and to overcome this, multiple transceivers need to be installed in OBU or RSU to allow multiple channels to listen in at one time (Eichler, 2007) and (Al-Hourani et al., 2014). However, there is only one transceiver in each vehicle for the deployment of DSRC.

As mentioned, Channel 178 is a control channel which is the most important and critical channel in DSRC. This control will be monitored by vehicles and RSUs and broadcasted messages and announcements will be monitored by the OBU. This control channel is only used for messages less than 200μs and if a message exceeds this, another channel must be used. This channel must be switched every 100ms and remain on for a minimal amount of time to receive safety messages. This is to allow the receiving of safety broadcasts from nearby vehicles and guarantees that messages are not sent before switching to the control channel. Besides that, the time switching channel must also be synchronized. This control channel also allows the vehicles to receive safety messages correctly without error, and to access the service of the network (Reddy et al., 2000) and (Sabouni & Hafez. 2012).

2.5.2 Wireless Access in Vehicular Environments (WAVE)

ITS is expected to be broadly applied in the foreseeable future to further enhance the transportation environment, and V2V communication (Ma, Chen & Refai, 2009), (Lott, Meincke & Halfmann, 2004) and (He et al., 2011). The WAVE spectrum allocation for applications are shown in Table 2.3 (Williams (2008), Li (2010)). WAVE technology comes as a great solution for ITS, to further improve the aspects of safety, intelligent management, as well as data exchange services.

Based and built upon the IEEE 802.11p standard, WAVE will be able to provide high speed V2V and V2I transmission of data, as it is the next generation of DSRC. WAVE notably differs from Wi-Fi and cellular wireless networking environments. Nevertheless, the WAVE uses the IEEE 802.11p standard, an expansion of IEEE 802.11, but it can be considered an entirely new architecture. WAVE technology fully implements the characteristics of IEEE 802.11a, IEEE 802.11e and IEEE 802.11q. IEEE 802.11p commonly uses channels of 10 MHz bandwidth in the 5.9 GHz band. Differing from 802.11a, the transmission time for a specific data symbol is doubled, and only half of the bandwidth is used. The characteristics of radio channels in vehicular communication environments can be adapted better by the receiver. Examples are signal echoes from infrastructures and vehicles.

In the Physical layer, the Control Channel (CCH) and Service Channel (SCH) are required to be monitored by WAVE devices. The role of SCH is to carry the IPv6 stack of data, while CCH is utilized for short WAVE messages used by safety applications, as well as service announcements. The MAC layer stations are able to deliver and obtain frames with Basic Service Set Identification (BSSID), that enables an area within communicable distance with fast moving vehicles to directly exchange data by using BSSID using the same channel

without paying extra penalties. This is due to the operation process of communication building based on traditional IEEE 802.11 that involves multiple handshakes and link building, as well as beacon scanning, making it complicated for road-vehicle environments as the link process should be completed in no time.

Although widely applied, WAVE is still arguably unstable when it comes to providing complete security to all road users, as the wireless environment is vulnerable, and not many architectures are yet suited to high mobility communication. Furthermore, it is being used on the roads where human lives are involved (Yin et al., 2006), (Ho et al., 2010). The system needs to be improved, until it is mature, and only then can it be suitable to include entertainment applications, etc.

Table 2.3: WAVE Spectrum Allocation for Applications

Country/Region	Frequency Band (MHz)	Reference Documents
ITU-R (ISM band)	5725-5875	Article 5 of Radio Regulations
Europe	5795-5815, 5855/5875-5905/5925	ETS 202-663, ETSI EN 302-571, ETSI EN 301-893
North America	902-928, 5850-5925	FCC 47 CFR
Japan	715-725, 5770-5850	MIC EO Article 49

2.6 VANET Characteristics

VANET applies the same theory and principles as the MANET, but VANET has its own unique characteristics, as follows (Rasheed, et al., 2017).

(a) High Mobility

VANET is used by moving vehicles, hence the nodes inside VANET are usually moving rapidly at random speeds. So, the positions of the nodes are always at random and hard to predict. VANET has a difficulty in measuring and predicting the movement speed and pattern of every motorized vehicle. The nodes in VANETs are constantly moving at a high velocity. This makes it harder for VANET to carry out prediction based on the node's position and improving the overall protection of privacy. An increase in the number of vehicles will result in a decrease in the average speed of vehicles. Hence, a more stable network and a decrease in the number of vehicles on the highway will result in an increase in average speed and most likely a less stable network will occur (Vaibhav, et al., 2017).

(b) Network Topology

The network topology is related to the high mobility of the nodes. If nodes are highly mobile, and they are moving at a random speed, the position of the nodes will change frequently (Vaibhav, et al., 2017), (Shah et al., 2018). However, maintaining routes is a very challenging task in VANETs due to fast moving vehicles and a lively information exchange. Vehicular nodes traveling from sender to receiver suffer from vast packet loss and delay due to congestion. To reduce the impact from the topology and the frequent changes, (Sailaja, Ravi

& Jaisingh, 2018) introduced the Ad Hoc On-demand Distance Vector Routing protocol (AODV) and the Early Congestion Detection & Control routing protocol called (EDAODV).

(c) Free Network Size

VANET is a type of network that can be implemented scaled from a small specific area, several cities to a whole country (Shah et al., 2018).

(d) Frequent Exchanges of Information

VANET is design for wireless environments, so the nodes are connected to exchange data and information among the other vehicles and RSUs. The ad-hoc nature boosted and motivated the information exchange between nodes, hence the information exchange between the nodes becomes frequent (Shah et al., 2018), (Hasrouny et al., 2017).

(e) Time Critical

The important information and data must be transmitted and received by the nodes within a time limit, so that decisions can be made, and action can be taken in time (Hasrouny et al., 2017).

2.6.1 Vehicular Safety Devices

Vehicular safety devices are designed to protect drivers and passengers from injuries in case of road accidents. There were also passive-restraint devices that will protect the drivers and passengers without the needs of performing an action of their part (Panjeta, Aggarwal & Student, 2017). These devices include:

(a) Airbags

Airbags are passive-restraint devices that do not need to be activated by drivers or passengers. It will automatically inflate on its own very rapidly during a heavy collision. The airbags will provide protection and prevent injury or death.

(b) Seatbelts

Seatbelts are the main protection that drivers and passengers can get from death or injury during a car crash. Seatbelts will hold drivers and passengers in their seats, preventing them from hitting the interior or diving through the windshield of the vehicle during a road accident (Ross, Sicking, Zimmer & Michie, 1993).

(c) Anti-lock Brakes

Anti-lock braking system (ABS) is an electronic navigator that prevents the vehicles' wheels from locking when the driver steps on the brakes. ABS let the driver handle the control of the vehicles at a more stable pace while on rough or wet surfaces and during emergency braking. Vehicles that lack ABS will have their front wheels locked during emergency braking which will cause the drivers to lose control of the vehicle (Ross et al., 1993).

(d) Electronic Stability Control

Electronic Stability Control (ESC) works alongside ABS by braking the vehicle and comparing acceleration, rotation and wheel speed with the intended direction of steering the vehicle. This ESC will assist the driver to regain the control of the steering on a slippery road or a high-speed turn (Ross et al.,1993), (Vuong, 2011).

(e) Traction Control System

Traction Control (TC), is designed to prevent loss of traction from the wheels. For example, on a wet and slippery surface, it will reduce the traction of the wheels and the road surface.

Hence, the TC will adjust the brake pressure to allow maximum contact between the wheels and the road surface. Without the TC, the loss of traction can be dangerous and even fatal (Tonkin et al., 2003).

2.7 Challenges of VANET

VANET might be useful and helpful to drivers, but there is one main challenge encountered by VANET, which is security. Security should be considered as the most important issue, especially in VANET (Nadeem & Howarth, 2014), (Harpreet & Supreet, 2015) and (Al-Kahtani, 2013). This is because the information being transmitted is usually important and critical. If this information is modified and not accurate, it may cause harm to drivers and other road users. VANET is vulnerable to many types of attacks such as DoS attacks, DDoS attacks, bogus information, ID disclosure and more.

Current research focuses on the security of VANET by providing different solutions to protect it from attacks. However, these solutions still need to be improved and upgraded to reach the level where drivers can travel in a safe environment without the VANET service being disturbed. However, this is not an easy task as there are potential attacks that also need to be considered. To achieve these high levels of security might take more research and time because security mechanisms usually involve more than one protocol or algorithm (VinhHoa & Ana, 2014).

The mobility in VANET is brought about by adapting characteristics of the wireless ad hoc network. VANET does not depend on the fixed infrastructure for communication and data transmission. The mobility of the nodes in VANET are medially compact and nodes are primarily moving vehicles. Due to the high mobility of VANET, the network topology changes frequently. However, VANET mobility models are predictable since the nodes are

restricted and only able to move on the roads and highways. VANET does not have to worry about power resources problems as in MANET (Rampaul, Patial & Kumar, 2016).

2.8 VANET Applications

There are two basic applications for VANET: the first is Safety Oriented Applications and the second is Non-Safety Oriented Applications. Non-safety applications are divided into two: pragmatic oriented applications and expediency-oriented applications. Safety oriented applications are essential in VANET due to the life saving factor. Safety oriented applications are developed to ensure safety of vehicles and passengers (Rampaul, Patial & Kumar, 2016), (Sinha & Mishra, 2013) and (Sudheera et al., 2016). Safety applications can help prevent road accidents. In detail, they allow the exchange of status information between the V2V and V2I.

Pragmatic oriented applications are commercial applications to give convenient service, for example internet access, real time video relay and so on. Next, expediency-oriented applications provide comfort to drivers and passengers. For example, peer to peer applications, where drivers can share music, movies and pictures on the network. Apart from this internet connectivity, drivers or passengers can access the internet all the time because VANET has provided constant connectivity to the user (Yan, Rawat & Bista, 2012). Table 2.4 shows the classes of application and their usage.

Table 2.4: Classes of VANET Application and Their Usage.

Classes	Application	Usage
	Real-time traffic	RSU stored real time traffic data and available to vehicles (Al-Qutayri, Yeun & Al-Hawi, 2010).

Safety Oriented		Solving problems in traffic jams, avoid congestion.
	Co-operative Message Transfer	Slow or Stopped Vehicle to exchange messages with others vehicle (Eze, Zhang & Liu 2014) Emergency braking to prevent accidents.
	Post-Crash Notification	Vehicle involved in accident spread warning message about its position to fall behind vehicles.
	Road Hazard Control Notification	Car notice other cars information about road curves and sudden downhill stretches.
	Cooperative Collision Warning	Warning driver's capacity under crash route.
	Traffic Vigilance	Input: Camera installed at RSU Tool against driving of-fences
Pragmatic Oriented	Remote Vehicle Personalization/ Diagnostics	Download and install personalized vehicle settings. Uploading of vehicle diagnostics.
	Internet Access	Through RSU, Vehicles can access internet.
	Digital map downloading	Traveller download map of regions for travel guidance.
	Real Time Video Relay	Traveller watch real time video.
	Value-added advertisement	Online and off-line advertisement to attract customers. For example, petrol pumps, 24 hours convenient store and so on.
Expediency Oriented	Route Diversions	During road congestions, route and trip can be planned.
	Electronic Toll Collection	Toll collection via application. Its will help both party, toll operator and vehicle drivers.
	Parking Availability	Search of availability of parking slots.
	Active Prediction	Expect the upcoming terrain (Burmester, Magkos & Chrissikopoulos, 2008)
	Environmental Benefits	AERIS research program produce and gain environmentally relevant real-time transportation data
	Time Utilization	Browse Internet or productive task during traffic jams
	Fuel Saving	Vehicle utilizes TOLL system application to pay toll without stopping, save fuel around 3%. (Raya & Hubaux, 2005)

2.9 Security Mechanisms in VANET

To create a secure VANET environment, there are four important security requirements that must be satisfied, which are confidentiality, integrity, availability and authentication. These will be discussed in detail below.

Confidentiality

In the first place, confidentiality can be defined as "confidential communication" (Nasir et al., 2013), (Chen et al., 2011), (Zhu et al., 2009) in VANET. In other words, the communication channel between the sender and receiver must be protected. The third party is not able to decrypt the message sent from the sender because the only specific group member in a certain communication channel has the key to decrypt it. In detail, every time a sender sends a message, it must be encrypted to prevent third parties from stealing the contents of the message (Yaqoob, 2017). In this way, the privacy of the sender and receiver is secure. To deal with privacy, the author (Chikhaoui et al., 2017) introduced a ticket-based authentication scheme for VANETs that relies on temporary tickets.

Integrity

In addition, integrity also become an important security requirement in VANET. Integrity for all messages sent over the VANET must be protected and secured in order to prevent a third party from altering and editing the content of the message (Mokhtar & Azab, 2015). To achieve integrity, data verification is required between the sender and receiver. In detail, first the sender vehicles must be authenticated, then after the authentication, the receiver vehicle does the data verification to check the data of the message. In this way, the data in the message is protected from malicious attackers.

Availability

The next security requirement is availability. In a traffic environment, VANET should be available at any time so that it can respond as fast as possible to whoever requested the information while driving. Besides that, availability must make sure all the information is available to legitimate drivers when they request it. The performance of the network should not be affected, and it should always be available even if it is under attack (Wagan & Jung, 2014), (Bariah et al., 2015).

Authentication

The authentication also is an important security requirement in VANET. Every transmitted message in VANET must be authenticated so that the authorization level of vehicles can be controlled. Besides that, authentication can make sure all the messages are created by legitimate users. Thus, all the messages in VANET are protected and secured (Chaubey, 2016).

2.10 Type of Attackers

Insiders or Outsiders

An Insider is known as a member node that can communicate with all other members of a network. An Insider is capable of attacking in various kinds of ways. An Outsider, on the other hand, has a limited number of methods for performing attacks due to the nature of not being validated to directly communicate in the network, with other members (Hussain & Oh, 2014), (Chaubey, 2016).

Active or Passive

An active attacker will launch its attack on the network by creating new packets that will cause damage to the communication. Passive attackers mainly stay stealthy by

eavesdropping on the communication channels to steal valuable information. (Patel & Jhaveri, 2015).

Malicious or Rational

A rational attacker anticipates his/her own interests from the attacks that they perform. Hence, these attacks are much more foreseeable as they follow certain patterns. In contrast, a malicious attacker implements multiple different techniques and methods to vandalize the network as well as the member nodes without deriving personal benefit from the attacks (Patel & Jhaveri, 2015).

Local or Network

Local attackers launch attacks on nodes on the same network. A network attacker or an extended attacker launches attacks across the network, scattered throughout the network by controlling several entities (Agrawal et al., 2013).

2.11 VANET Attacks and Impact

There are many possible security impacts of VANET attacks, (Azees, Vijayakumar & Deborah, 2016), (Liang et al., 2015) and (Azogu et al., 2013). Figure 2.9 shows these potential predicted impacts in VANET networks along with different types of attack.

2.11.1 Low Impact Attacks

The black hole attack, ID disclosure, cheating their position, monitoring attack and social attack can be classified as low impact attack threats as they will not cause severe network interruption and do not bring down the network. All the attacks under this category will interrupt the beginner level attacks (Azees, Vijayakumar & Deborah, 2016), (Liang et al., 2015) and (Azogu et al., 2013).

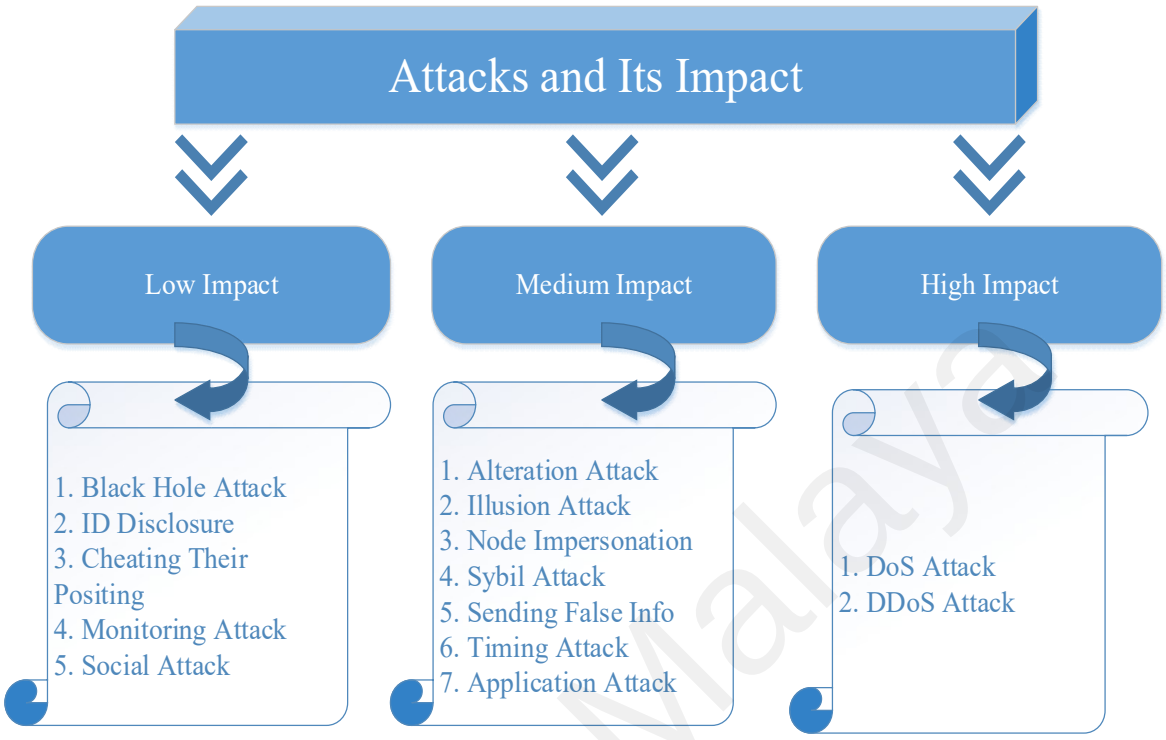

Figure 2.9: Taxonomy of Attacks and Their Impacts

(a) Black Hole Attack

In a black hole attack, attackers will find the shortest path to the target nodes or victims that they want to attack or intercept. The attacker node will transmit a path response packet to the target node. Nonetheless, the attacker node will receive the request from the victim nodes before the actual nodes reply to it. Hence, a new malicious route will be created between the attacker node and victim node. After this malicious route is created, attackers can decide whether to transmit the packets to unknown destinations or drop all the packets (Mishra et al., 2011), (Zaidi & Rajarajan, 2015) and (Razzaque, Salehi & Cheraghi, 2013). So, the packets sent by the victim nodes will never reach their destinations. An example of the black hole attack is shown in Figure 2.10.

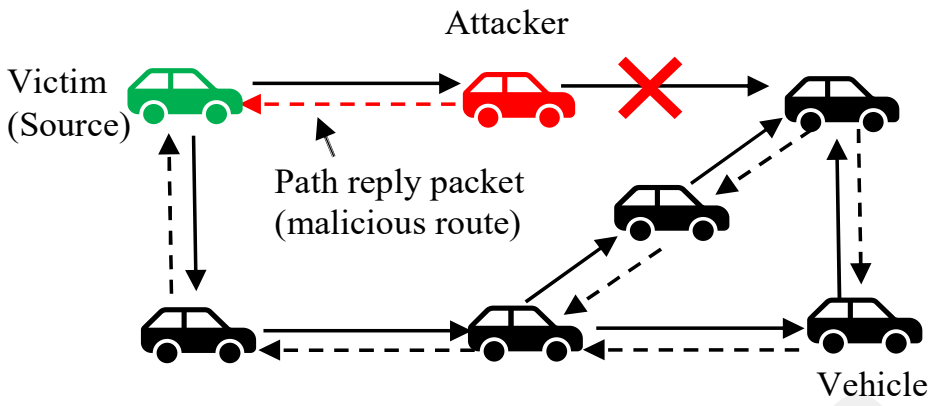

Figure 2.10: Black Hole Attack

(b) ID Disclosure Attack

In an ID Disclosure, the attacker will attack vehicles through the RSU. It is considered as a passive attack because the attacker will target all the other nodes in the network instead of the intended victim. When the nearby neighbour nodes are being attacked, they will take up the ID of the intended victim node and their locations (Razzaque, Salehi & Cheraghi, 2013), (Elsadig & Fadlalla, 2016) and (Gillani et al., 2013). By doing so, the attacker can track the current location of the victim's node easily. An example of the ID disclosure attack is shown in Figure 2.11.

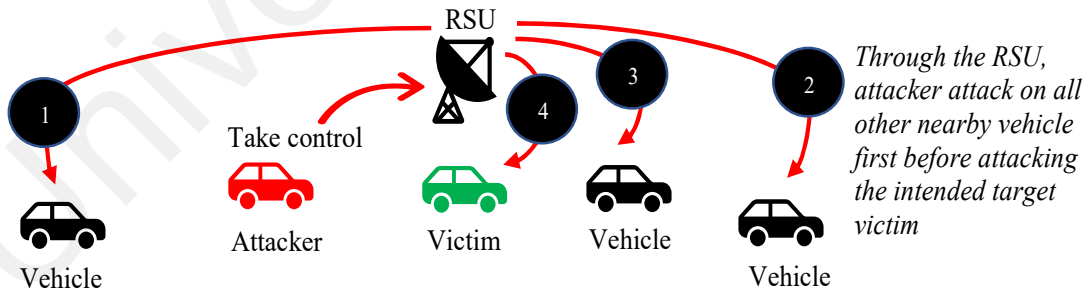

Figure 2.11: ID Disclosure Attack

(c) Cheating Position Attack

Cheating position attack is intended to create an illusion of another different vehicle that is moving normally like the other vehicles along a pre-set route, and it is difficult to detect.

This cheating position can use single ID or multiple IDs. Single ID cheating position uses only one virtual ID while multiple IDs use multiple virtual IDs on the pre-set route. This cheating attack is used to manipulate the traffic situation by creating an illusion of positioning and movement (Gillani et al., 2013). While creating an illusory pre-defined route, the attacker will keep the pre-defined position to stay within his network range to make it hard to be detected. Examples of the attack are shown in Figure 2.12 and Figure 2.13.

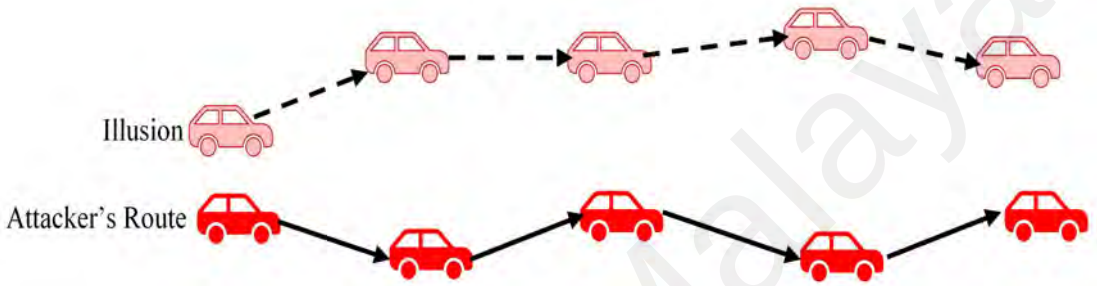

Figure 2.12: Cheating Position Attack Using Single ID

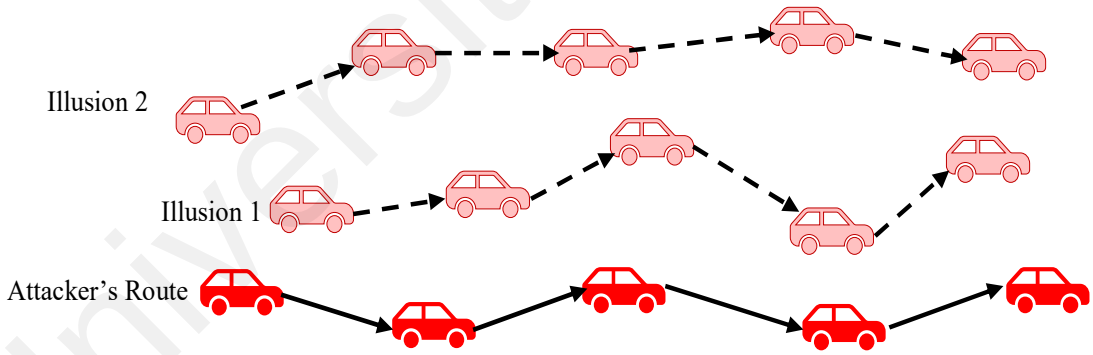

Figure 2.13: Cheating Position Attack Using Multiple ID

(d) Monitoring Attack

In motoring attacks, the attacker will not directly attack the other vehicles or nodes. Instead, they just monitor the network and listen to the communication among the vehicles and RSUs (Eze et al., 2016), (Raiya & Gandhi, 2014) and (Mehta, Malik & Bajaj, 2013). Monitoring attacks can also be considered as eavesdropping. The most well-known monitoring attack is

the Man in the Middle Attack. For this attack, the attacker will take control over the communication between senders and receivers without them being aware. The attacker can either listen to them or insert false information into the communication. An example of the monitoring attack is shown in Figure 2.14.

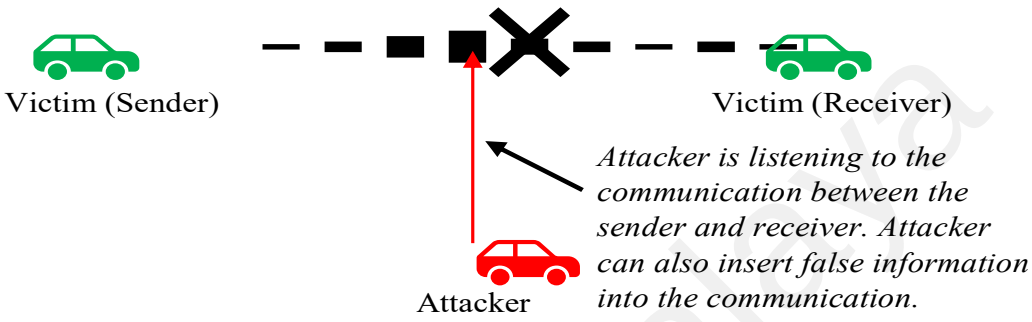

Figure 2.14: Monitoring Attack

(e) Social Attack

A social attack is intended to send immoral or vulgar messages to other vehicles. The intention of this attack is to create unwanted problems for other road users. When drivers receive these messages, they may get angry. The objective of the attacker is to instil negative behaviour in the drivers (Vaibhav et al., 2017). An example of the social attack is shown in Figure 2.15.

Figure 2.15: Social Attack

2.11.2 Medium Impact Attacks

The alteration attack, illusion attacks, node impersonation, sybil attacks, sending false messages, timing attacks and application attacks are all classified as medium impact attacks. All attacks under this category are medium impact because only the communication can be affected, but all the nodes still can send\receive the messages and continue as part of the network (Tangade & Manvi, 2013), (Manvi & Tangade, 2017).

(a) Alteration Attack

Alteration attacks occur when attackers delete, insert or make changes to the original messages without the authorization yet appear legitimate. In this attack, the alteration is not only applied to the message itself, it also alters the code in it. Alteration attack is also very difficult to detect (Kaushik, 2013). An example of the message alteration attack is shown in Figure 2.16.

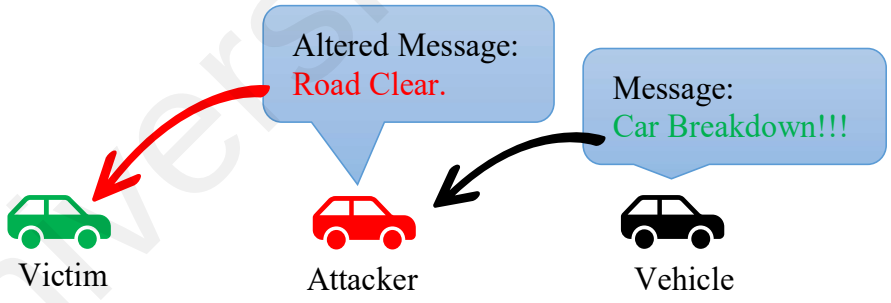

Figure 2.16: Alteration Attack

(b) Illusion Attack

The illusion attack makes the victim believe the fake messages sent by the attacker. The idea of this attack is to create fake traffic messages that seem believable to the victim. The victim will then change his driving behaviour according to the fake traffic messages. The attackers achieves his goals in the end (Faezipour et al., 2012), (Nema, Stalin & Lokhande, 2014).

This attack will have an impact on both the physical components and the network itself. This attack scales from a simple prank to a full-blown terrorist attack. An example of the illusion attack is shown in Figure 2.17.

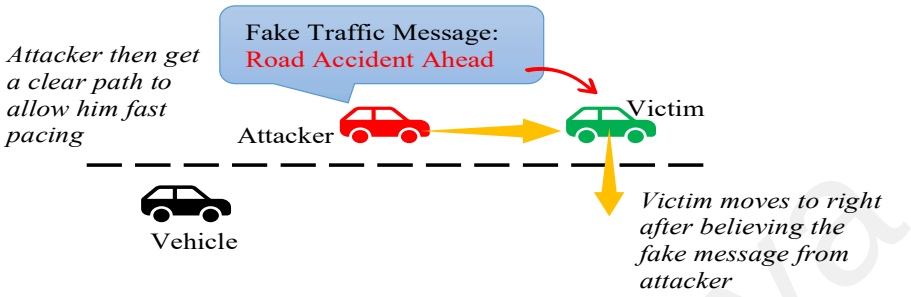

Figure 2.17: Illusion Attack

(c) Node Impersonation Attack

As we know, each vehicle has its own unique ID that is used to identify the specific vehicles in VANET. During a road accident, the vehicles involved can be located by detecting the ID through the network. In a node impersonation attack, attackers will alter their ID and pretend to be the originator. The attacker receives the message from the originated vehicle that broadcast the message, modifies the message content then sends it to the other vehicles. In node impersonation, the attacker is trying to masquerade as the legitimate sender (Ghaleb, Razzaque & Isnin, 2013), (Sari, Onursal & Akkaya, 2015). The attacker can also pretend to be the RSU that sent the false messages. Node impersonation attacks prevent the identification of vehicles during collisions, as shown in Figure 2.18.

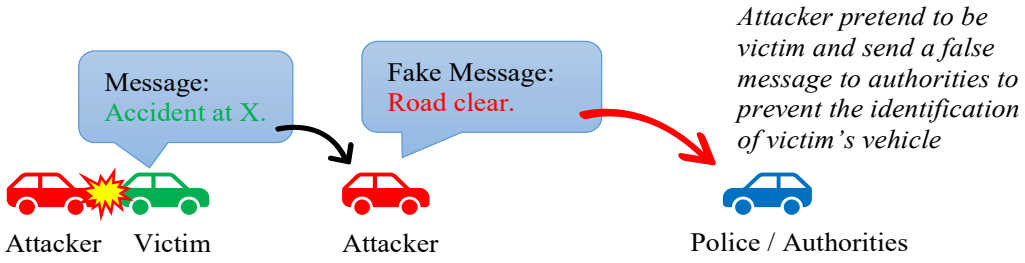

Figure 2.18: Node Impersonation Attack

(d) Sybil Attack

In a Sybil attack, an attacker pretends to be multiple vehicles at different locations with different IDs at the same time. The objective of the attacker is to transmit multiple messages to the other vehicles using the different IDs. Through this attack, the other vehicles will believe that the messages coming in are legitimate and there is heavy traffic up ahead. A single false messages transmission may not seem convincing enough, but if the false messages come in bulk, the other vehicles will believe that the messages are real (Kumar & Sinha, 2014). The Sybil attack is considered one of the most critical attacks as it may harm the network system and topology. An example of the Sybil attack is shown in Figure 2.19.

The attacker pretends to be multiple vehicle at different position and broadcast fake messages to other vehicles.

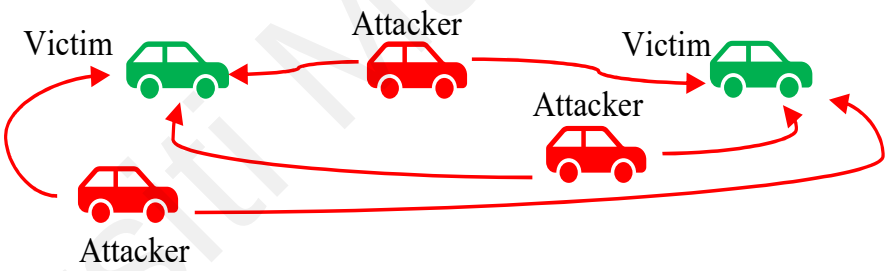

Figure 2.19: Sybil Attack

(e) Sending False Information

The idea of sending false information to other vehicles is to make movement on the road easier for the attacker. This is usually done for personal advantage. For example, the attacker sends false information such as "Heavy traffic up ahead" to other vehicles. So, the other vehicles that received the false information will try another alternative route to avoid the fake heavy traffic which allows the attacker to move at fast pace easily (Kumar & Sinha, 2014), (Alexiou et al., 2013). An example of this attack is shown in Figure 2.20.

Figure 2.20: Sending False Information

(f) Timing Attack

Timing attacks can be dangerous and critical for some scenarios, especially when there is a road accident up ahead. When the attacker receives a message regarding a road accident up ahead, instead of forwarding the message to other vehicles, the attacker creates a delay time slot into the original message which made the other vehicles received it later than they should. Supposedly, the nearby vehicles should get the notify message right after the road accident happened, but the attacker had delayed the message to be sent to the others (Mejri, Achir & Hamdi, 2016), (Gadkari & Sambre, 2012). An example of the timing attack is shown in Figure 2.21.

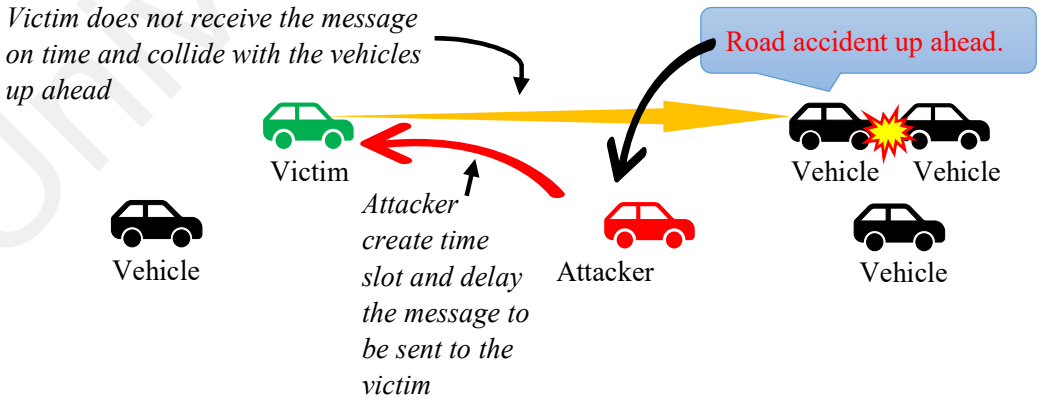

Figure 2.21: Timing Attack

2.11.3 High Impact Attacks

Last but not least, the DoS and DDoS classified as high impact (Wasef et al., 2010), (Seuwou et al., 2012) Under a DoS attack and DDoS attack, each time an attack takes place, the entire network is not available for legitimate users. However, the entire network regenerated the effort to deliver continuous service. The service is only accessible for a short time before its breakdown and all other services in the network will be unavailable.

(a) Denial of Service (DoS) Attack

In a DoS attack, the intention is to cut off the VANET service access of the victims. DoS attacks have always been the most critical attack not only in VANET, but in every scenario that involved networking (Seuwou et al., 2012). For this attack, the attacker will have sent high amounts of fake or dummy messages to overload the network channel. The attacker can launch this attack and send fake messages not only to the victim, but also the RSUs to overload the whole network (Liang et al., 2014). The main aim of the DoS attack is to engage the resource as well as prevent the legitimate VANET user to access the resource (Deshpande, 2013) and (Tyagi & Dembla, 2014). The user is unable to get the updated message on time, and it will lead to unnecessary accidents. DoS attacks can have a large impact on the VANET environment. An example of the DoS attack is shown in Figure 2.22.

The wide-ranging consensus on tackling DoS attacks is to direct data or packets whose size or content is unusual, this has the outcome of causing unforeseen reactions in the network, up to the disruption of service (Jeffane & Ibrahimi, 2016). Several network parameters recommend that there might be a DoS attack against the network controlled by the attacker. To safeguard drivers' safety amongst mischievous nodes, a novel system for forecasting automotive accidents in V2V networks uses the Received Signal Strength Indication (RSSI).

The system offers real-time crash avoidance from mischievous or misbehaving nodes. In the VANET network, it will boost driving security as well as sustaining other applications and vehicles periodically with safety messages about their precise position sent to its neighbours.

In VANET environments, normally the DoS attacks the transmission channel to affect the channel jam. The major reason is to block the genuine nodes from gain access to the network essential services. Network sources and node will not be capable to obtain or transmit crucial data or information because of the DoS attack. The network systems remain therefore no extensive accessible to genuine users. DoS shall not be permitted to occur in VANET, for the reason that it's a life essential information that must get its destination fast and on time. There are three type of DoS attack, namely packet dropping, jamming channels and oppressing the node resources.

Packet Dropping occurs once the attacker selectively drops packets from the network. Packets might have valuable data for the official receiver and remain held back with the attacker to use them over again at another time. The objective of such an attack would be to avoid registration and insurance authorities from realizing about accidents affecting a vehicle and to prevent dispatching accident reports to RSUs. The RSU is an access point, utilized simultaneously with the vehicles, to permit data or information distribution on the highways or roads.

Jamming the Channel happens when the attacker jams all the channels so that users cannot access or enter the network and channel. Jamming channels is the worst case scenario in DoS attacks. Attackers will send high frequency messages to jam the channel, and this will stop the nodes between users from sending and receiving, making services unavailable.

Finally, in the Oppress the Node Reserves DoS attack, the attacker aims to crush node sources such that the nodes cannot execute further crucial and essential responsibilities. entire resources of the nodes will be constantly engaged in message authentication, which is going from attacker connections. A totally wrong message will be received by the user.

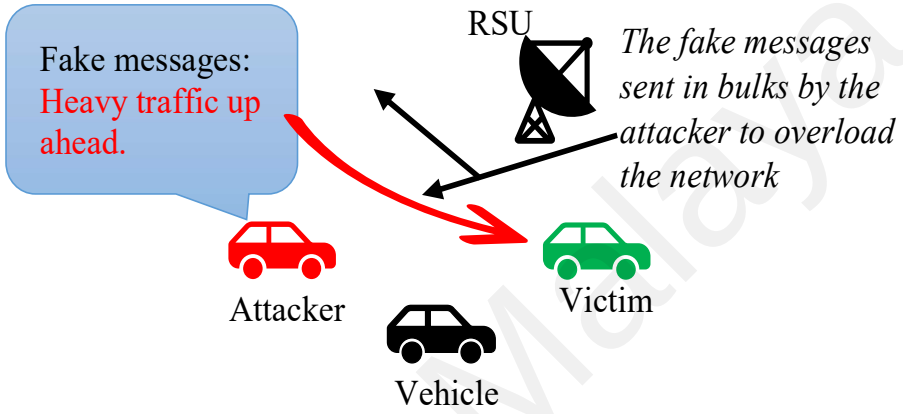

Figure 2.22: Denial of Service Attack

(b) Distributed of Denial of Service (DDoS) Attack

The DDoS attack is a distributed form of DoS attack and is more severe and catastrophic compared to the DoS attack. Essentially, a DDoS attack is launched by a few attackers from different locations at different times to overload the network as with a DoS attack. The victims of a DDoS attack will have their network overloaded and be unable to communicate with the other vehicles and the RSUs (Torre, Rad & Choo, 2018), (Hamida, Noura & Znaidi, 2015) and (Rasheed et al., 2017). An example of the DDoS attack is shown in Figure 2.23.

The information transmitted over a vehicular network is sensitive and can affect important safety decisions. However, they face various types of security attacks, such as DoS attacks and DDoS attacks, which are a rapidly growing problem and require much consideration

because such attacks do not require the penetration of the target network (Kim, Kim & Shim, 2014). Consistent communication in VANET is important to provide functional and reliable traffic safety and efficiency applications. Security is the major issue in the network due to the mobile nature of the vehicles. There is a need for a novel traffic congestion detection and removal scheme against DDOS attacks. The attacker's behaviour is broadcasting the huge numbers of false information packets in networks (Pathre, Agrawal & Jain, 2013). Some of the DDoS attack detection methods are shown in Table 2.5.

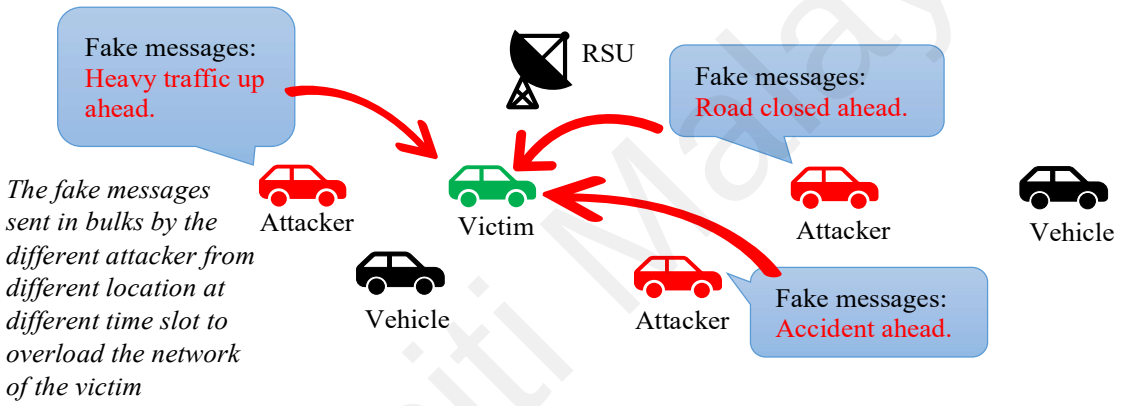

Figure 2.23: Distributed Denial of Service Attack

2.12 DoS History in General

A Denial-of Service attack (DoS) is one of the worst security threats in networking and prevents legitimate users the right to access the network. Based on the Figure 2.24, we can see that an attacker will usually control a server or computer, that sends out requests to servers or computers to flood a single target with multiple requests. An authorized user will not be able to interact with the target due to the target computer being flooded with traffic generated by the attacker. The are 3 main DoS detection methods. The first is Mirrored Data Packets (MDP). MDP provides a complete description for full analysis, even when it is not operating on the flow of traffic. It can also detect abnormality or irregularity quickly. The second method is Analysis of Packets. This method involves a mitigation device that can

detect irregularity in an instant and continuously processes all incoming and outgoing traffic. Finally, there is Flow Sampling. Flow sampling involves the router testing for packets, and transferring a datagram containing the packet's data. This is one of the most popular choices due to its high scalability.

The first documented DoS-style of attack was launched in 2000, in the second week of February, by a hacker known as "Mafiaboy". Mafiaboy successfully shut down the World Wide Web (WWW) for approximately a week. More than 50 e-commerce sites were affected, including Amazon, eBay, Dell and CNN. The damage caused by this 15-year-old Canadian Hacker was estimated at $1.7 billion by the U.S. Federal Bureau of Investigation (FBI). This changed the dynamic of the Internet in the US Government's eyes. Before the attack, the Internet had only played a limited role, in research and the economy. The scale of the damage showed that the Internet had become essential to the workings of many governments and economies. Cybercrime had since been transformed from an individual issue to a matter of national security (Ismail, Aborujilah, Musa & Shahzad, 2013).

Although the previous case was the first documented DoS attack, the first ever DoS attack can be traced way back to 1974 and interestingly (Gregory & Glance, 2013), it was also launched by an underaged teenager. David Dennis, a high school sophomore from Illinois shut down 31 users' systems at a time simply because he was curious about what the command "ext" can do. He was exposed to programming from the Computer-Based Education Research Laboratory (CERL) at the University of Illinois Urbana-Champaign. The "ext" command was meant to allow external devices to interact with the system, without the external device, the terminal of the system would lock up, and users had to shut the system down and turn it on again for the system to function.

Dennis hence wrote a simple program that sends “ext” commands to many PLATO terminals which were a very new computerized shared learning system at that time, eventually shutting down 31 systems. In the mid to late 1990s, simple bandwidth-based DoS Attacks and chat floods were used by hackers to gain administrator privilege controls in Internet Relay Chat (IRC) when it started to take off. When the administrator logs off the channel, they will lose control of the channel, so the hackers will send these attacks to force everyone, including the admin, to log off the channel, and then to take control of the channel. Besides the aforementioned cases, below are the other famous DoS/DDoS attacks in history. As Distributed Denial of Service is an enhanced form of DoS attack, we will be discussing them all together.

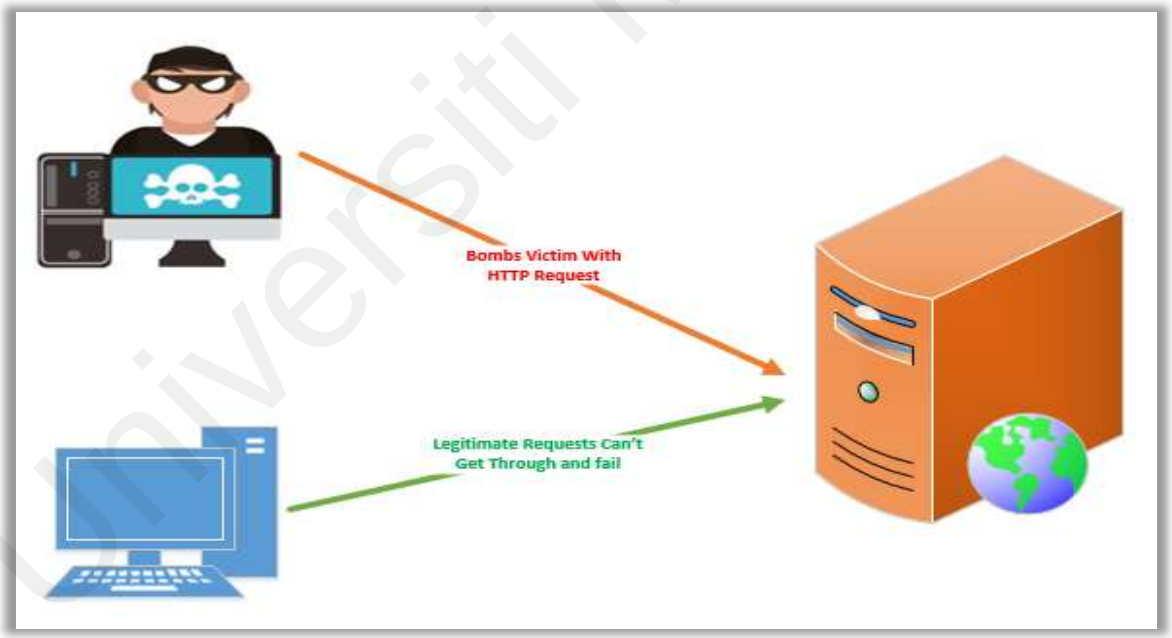

Figure 2.24: General DoS Attacks

April 2017 saw the world's first cyberwar. The entire government, financial and online media services of Estonia were shut down because of a DDoS attack. It was rumoured to be launched by the Russians and at the same time, the official sites of Estonia were swamped with large amounts of media content. This attack has had a huge effect on Estonia, as the country was operating in paperless mode, from managing the government to finance at the time.

In the January 2008, Project Chanology: Social activism launched a DDoS attack on the Church of Scientology together with other malicious acts such as sharing documents, pranks, pickets and information campaigns online regarding the Church. In the Fall and Winter of 2012 and 2013, Operation Ababil took place. At least 26 banks in the US were targeted by a group called the Izz ad-Din al-Qassam Cyber Fighters in revenge for an anti-Islam video. This DDoS attack shut down major banks such as Bank of America, Citibank, PNC bank and more. It is considered less severe compared to today's attacks, however this attack was still able to knock out most bank operations for 6 months. In August 2016, Mirai was discovered to be the mastermind behind many Internet of Things (IoT) devices attacks for the past years, buying using the internet, searching for vulnerable devices, and infiltrating using common factory default credentials to infect them. In October of the same year, the Dyn attack was launched. It disrupted websites including NEtflix, Reddit and Twitter, it was the biggest DDoS attack of that time. The DDoS attack on GitHub on the Morning of 28th February 2018 marked the biggest DDoS attack of all time, and peaked at 1.3Tbps, affecting 20 million global users. On the next morning, GitHub was hit by a second wave of DDoS attack, which lowered the availability of the website by 65%, twice the day before (25%), and the geographical scope was also widened, but it was immediately mitigated in 15 minutes (Mansfield, 2015).

2.13 DDoS History in General

A DDoS attack happens when somebody uses a network or multiple networks of computers to deny a service that people are using, usually for malicious purposes. The person with intent to cause harm will normally flood the targeted network with a great amount of useless requests using the computers that he/she controls all at the same time. There are other ways to carry out a DDoS attack, such as the shrew attack and slow read attack, but flooding the network with requests is more common. DDoS attacks cause users to be unable to use a resource that would otherwise be available to them. The reason behind this is normally for malicious intent, such as extorting money from a target company or from people. Sometimes, the people behind the attacks are youngsters who are just doing it for their own amusement. Figure 2.25 shows a diagram of common DDoS attacks.

Can we stop DDoS attacks? The answer is yes, and the system administrator or network engineer need to take immediate action on threat detection to prevent the damage from getting worse. There are some methods to identify a DDoS attack and there are also a few methods to detect DDoS attacks in the early stage. Once the DDoS attack hits the network, it will take some time to realize whether it is a DDoS attack. The DDoS attack normally will disturb the services without failing the server or application. Normally there is a command in the server to identify whether DDoS attacks have happened or not. In the command prompt one needs to type “netstat -an”. The standard output will display as shown in Figure 2.26. You may see numerous dissimilar IP addresses connected to specific ports. Now have a look at Figure 2.27 to identify the DDoS attack pattern. If the server has been attacked, this pattern is captured from the server using “netstat -an” (Pathre, Agrawal & Jain, 2013).

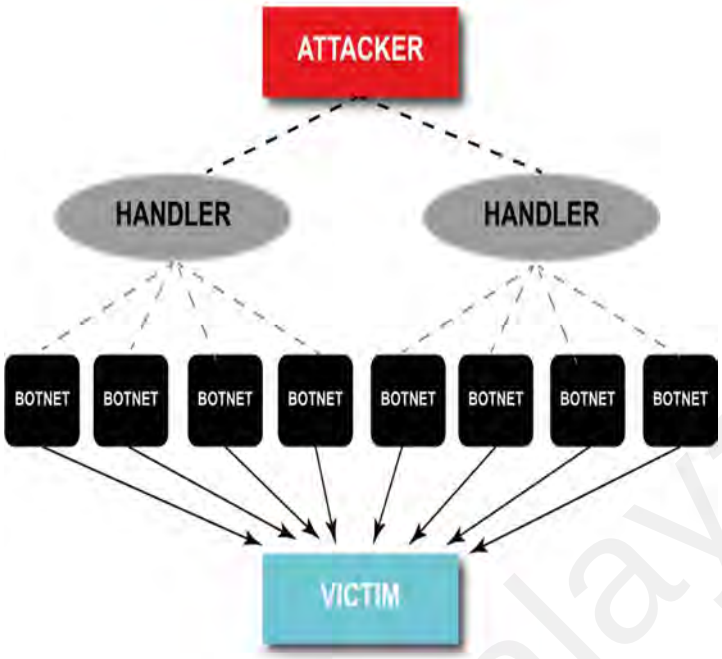

Figure 2.25: Diagram of DDoS Attack

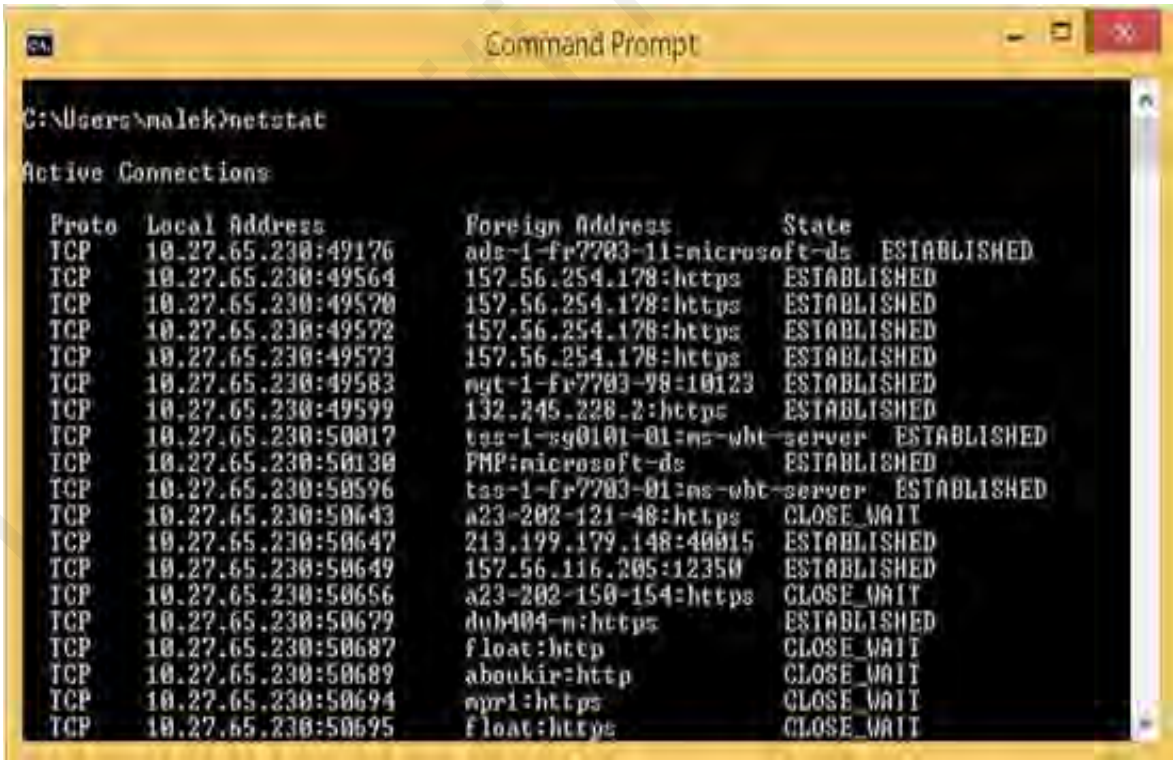

Figure 2.26: Standard Output Before the Attack Using "netstat -an"

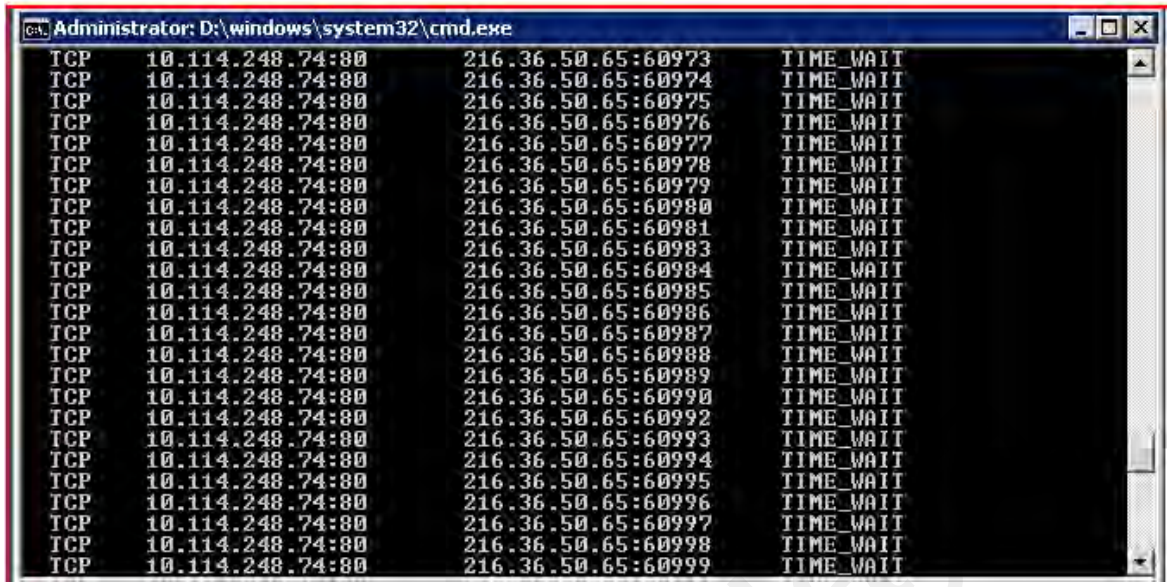

Figure 2.27: Standard Output During the Attack Using "netstat -an"

2.14 State of The Art of DoS and DDoS Attacks

This section reviews the background research on DoS and DDoS Attacks in several domains. The related research has been categorized into 5 categories, as follows:

1. DoS Attacks and DDoS Attack Detection Methods in VANET.
2. DoS and DDoS Attack Detection Methods Based on Networks.
3. DoS and DDoS Attack Detection Based on the Cloud.
4. Cluster-based DoS and DDoS Attack Detection Methods.
5. DoS and DDoS Attack Detection Methods Based on MANET.

The purpose of this study is to create a set of beneficial requirements that will be used to effectively understand the literature on the detection of DoS and DDoS attacks. The taxonomy of the DoS and DDoS attack detection methods is shown in the Table 2.5.

Table 2.5: Taxonomy of DoS & DDoS Attack Detection Methods

Attack Detection Methods				
VANET	**Network**	**Cloud**	**Cluster**	**MANET**
Sentinel: Defense Mechanism (Biasi, Vieira & Loureiro, 2018)	Radial Basis Function (RBF) (Karimazad & Faraahi, 2011) (Bhuyan et al., 2013)	Ensemble Based Multi-Filter Feature Selection method (Osanaiye et al., 2016)	Greedy Algorithm (Andrysiak, Saganowski & Choraś, 2013)	Cross-Layer Approach for Malicious Packet Dropping Detection (S'nchez & García, 2012)
The DDOS Attack Detection and Prevention in VANET by Group Controlled Analysis Model (GAC) (Vipin & Chhillar, 2018)	Honeypots Detection Methods. (Naik, 2015)	Trilateral trust-based defence mechanism against DDoS attacks (Iyengar & Ganapathy, 2015)	Safe Weighted Clustering Algorithm (Amine, Nasr-Eddine & Abdelhamid, 2015)	Identify the malicious using Response Sequence Packet (Rseq) and Code Sequence Packet (Cseq) (Dhaka, Nandal & Dhaka, 2015)
Queue Limiting Algorithm (QLA) ((Sinha & Mishra, 2014))	Packet Identification Anomaly Detection (PIDAD) (Thang & Nguyen, 2016)	Hybrid Intrusion Detection System (H-IDS) (Cepheli et al., 2016)	Advanced Marking Scheme (AMS) (Gupta, Joshi & Misra, 2012).	Fuzzy based Intrusion Detection (Balan et al., 2015)
Attacked Packet Detection Algorithm (APDA) (RoselinMary et al., 2013)	Botnet-Based Detection Approaches (Gibbs, 2014)	Group Testing Technique (Thai et al., 2008)	Clustering and Data Reduction based DDoS (Zhong, & Yue, 2010)	Clustering reputation mechanism to identify the flooding attack (Kaur, Toor & Saluja, 2014)
Protection Node Based Strategy method (Deepali. et al. (2015)	Network Intrusion Protection System (Wang et al., 2010)	DDoS resistant Augmented Split-Protocol (Rawal, Ramcharan & Tsetse, 2013)	Network Abnormal Feature Value (NAFV) (Chen et al., 2019)	Enhanced Adaptive Acknowledgement (EAACK) (Shakshuki, Kang & Sheltami, 2013)
A Novel Security Approach for Data Flow and Data Pattern Analysis to Mitigate DDOS Attacks in VANETs (Kaur & Mahajan, 2015)	Naive Bayes Classifier (Sharma & Mukherjee, 2012)	Signature-Based Detection Approaches (Zeadally et al., 2012)	Genetic homomorphic encryption algorithm (Elhoseny et al., 2016)	Distributed Scheme of Emerging Authentication and Intrusion Detection (Deny & Sivasankari, 2011)
Novel Traffic Congestion Detection and Removal Scheme Against DDoS Attack (Pathre, Agrawal & Jain, 2013)	Anomaly-based intrusion detection using - signal-to-interference-plus-noise ratio	Entropy based anomaly detection system (Navaz, Sangeetha &	Signature-based classifiers (Chaabouni et al., 2019)	Local Protection Nodes (LPN) and Remote Protection Nodes (RPN). The method is based on Security-Aware Routing

	(SINR) (Fragkiadakis et al., 2015)	Prabhadevi, 2013)		protocol (SAODV) (Xiang et al., 2011)
Classification of DDOS Attacks in VANETs based on Distributive Collaborative Framework. (Pavan , Sarma & Reddy, 2019)	Anomaly Based Network Intrusion Detection System (A-NIDS) (Van, Thinh & Sach, 2017)	CS_DDoS system ((Sahi et al., 2017)	Source-based anti-DDoS technique (Nguyen, Lin & Hwang, 2018)	Anti-Black hole Mechanism (Su, 2011)

2.14.1 DoS and DDoS Attack Detection Methods in VANET

Author (Sinha & Mishra, 2013) used Dedicated Short-Range Communication (DSRC) and revocation techniques. The detection method is constructed on the offender transferring or sending a message to the target node and then to different locations and may also have a diverse time slot for transferring the message, and the offender will attempt to modify the time slot and the message for different vehicular nodes. However, the main reason for the attack is to make the network inaccessible to the victims or vehicle nodes by bringing the entire network down. It has seven channels in DSRC, and four classes were created and sorted based on precedence. Class 1 represents the highest, while Class 4 the lowest. Nevertheless, some node in the VANET infrastructure will receive a restricted amount of security messages at a specified timestamp, so it is considered as the node that has already been attacked. In this way, it can safeguard itself against any DoS and DDoS attacks. The Queue Limiting Algorithm (QLA) introduced by (Sinha & Mishra, 2014) also uses similar schema to safety channels of DSRC to protect the lives of drivers on the road. According to the classification, the safety message will trigger first because the safety message is set at a high priority level. In this technique, each vehicle has a restricted size limit for receiving safety messages.

Group Adaptive Controller-based Method (GAC) introduce by author (Vipin & Chhillar, 2018). This method can detect a DDoS attack in VANET environments, and some communication can be lost because of heavy traffic flow. The simulated group will be generated by this method (Vipin & Chhillar, 2018). The method will consider the position and mobility of the vehicle. The speed of the vehicle, position and direction of the vehicle is considered by the group formation. The group of the centralized node is deliberate for the controller node in VANET. The controller can witness the communication between car and network. The communication analysis reflects the response time, communication delay and communication loss. In the end, this method identifies the adaptive node from the parameters of the vehicular network. The analysis will classify the node as safe or unsafe. The simulation is done with 50 nodes and the throughput result is 75%, the PDR ratio is 87% and communication loss is 0.83%.

According to the proposed schema the Local Protection Node (LPN) is selected from the hierarchical architecture (Bansal, Sharma & Prakash, 2015). The PDR value and threshold value will be compared, and if both values are equal then the monitor mode message transmits through the LPN and to other vehicles in the network for the purpose of sensing. If any vehicle that injects a large number of false packets is detected as an attacker, packets will be categorized as malicious nodes and discarded. Another similar method is the Protection Node Based Strategy (Deepali. et al., 2015). This will reduce the effect of DoS and DDoS attacks in VANET. The node is divided into multiple levels. Lower level nodes are used to protect the same level neighbouring nodes and the node is considered as a Local Protection Node (LPN). Whenever an attack happens the Remote Protection Node (RPN) will produce the protection node. RPN will filter the node, and if its malicious, then the Attack Notification Message (ANM) will be broadcast to other nodes warning them of the

malicious node. This technique reduces the effect of DDoS attacks, but it will take some time for the whole process for mitigation.

The Attacked Packet Detection Algorithm (APDA) (RoselinMary et al., 2013) and the Malicious Node Detection Algorithm (MVND) (Ghorsad et al., 2014) were introduced to detect DoS and DDoS attacks. The APDA method considers time stamp, position and velocity to detect the false nodes or malicious node. if this method detects the malicious node before the verification time, it will reduce the overhead delay for processing to improve security in VANET. However, the MVND method is used to detect malicious nodes before the verification time by using a hybrid network. The MVND method will first distribute the cluster keys by allocating an initial distrust value to determine a threshold value using standard deviation and will collect the behavioural data to determine whether the vehicle is abnormal or modified. If it is detected, then it will isolate the vehicle from the network. (Deepali. et al., 2015) also proposed a packet detection algorithm (APDA) to detect and identify DoS attacks in VANET. This method not only detects the attack but it verifies and limits the nodes that enter the network.

Another potential method to detect DDoS attacks in vehicular communication is the novel traffic congestion detection and removal scheme (Pathre, Agrawal & Jain, 2013). Reliable communication is really important in VANET to make available efficient and consistent efficiency and traffic safety applications. Some attackers intentionally broadcast vast numbers of false message packets in the network. In this method the false message is referred as an “Abstract Node”. In the normal traffic situation, with congestion and jams happening, the information will go to RSUs and the RSUs should detect and omit them continuously from the network. By using this method, the packet will be detected, and it will identify the attacker. Once the false information is in the network then all the other vehicles will re-route

according to the false information. This method will control the false information and the performance of the attacker will be reduced. The author did not reveal anything about the overall throughput and detection time. If there is an attack, some control packets delivered on time which is 37secs, focusing on 2 metrics only (Control packet analysis and traffic behaviour).

The current Sentinel (Biasi, Vieira & Loureiro, 2018) is a new defense mechanism to detect flooding attacks by time series analysis, by packet flow and mitigates the attack by creating a flow tree to find out the source of spoofed packets. Technically the authors divided the results between the detection rate of victim vehicles and the efficiency of the mitigation method. The algorithm can mitigate the attack flow in different parameters. Sentinel reached an average mitigation rate of more than 78% in all density scenarios and the system cannot increase the packet delivery ratio. The detection time is around one second and the detection time is increasing. Only two performance metrics were discussed by this paper. Author (Kumar, Sarma and Reddy, 2019) is also discussed similar mechanisms with sentinel defense mechanism. Author introduce Distributed and Classification by Pattern based Framework (DCPF). It will detect DDoS attack in vehicular environment. The proposed model will work on intrusion detection on vehicular communication through ISP via vehicular communication. In this model each and every node will consist of virtual protection ring to exchange data and for detection purpose the author used real world knowledge-based data set. The outcome of this work is produced better result and low overhead in the vehicular environment.

The author (Kaur & Mahajan, 2015) uses a different framework to mitigate DDoS attacks by using packet and location analysis to verify the attacker node and in sort to stop the data

produced from the attacker node. Nevertheless, model is called as Novel Security Approach for Data Flow and Data Pattern Analysia to Mitigate DDoS Attack in VANETs and the model is by (Kaur & Mahajan, 2015). The recommended model retains to been created to identify and alleviate the DoS and DDoS attacks in the VANET clusters to prevent several of the misconduct or mis-happening in the form of VANET node collapse, collision or in several form. In case the anomaly is discovered in the data communicated by the attacker connection, the connection is marked as the DDoS node and all new nodes in the cluster are notified regarding the attacker node and stop accepting data from that node. Moreover, the permanent nodes will connect with each one in the cluster. Assume that permanent nodes A, B and C are situated from East to west separately. Consequently, if a motor vehicle joins the coverage of permanent node A to permanent node B, it is noticeable that the motor vehicle is running in a parallel route. The attacker nodes would be analyzed by the middle node. The experiment is on a small scale and focuses on 4 performance metrics (PDR, End to End Delay, Throughput & Packet Drop). The author did not justify the amount of time taken for attack detection.

To detect the DDoS attack in VANET environments, (Biswas, Mišić & Mišić, 2012), came up with the Wireless Access in Vehicular Environments (WAVE) enabled VANET through synchronization-based DDoS attack detection. Meanwhile, broadcast communications in VANET networks does not have acknowledgements. In the periodic broadcast the sender and receiver will not know about the attack. Periodic frames will be broadcast by RSUs through transmitted WAVE announcements or Wireless Short Message Protocol (WCMP) on CCH at the consistent interval time for some service. In this model the attacker will try to coordinate the RSU's periodic transmissions and will convey the frame which will strike the

RSU's edge or frame. Two kinds of synchronization need to be achieved by the attacker to launch the attack: backoff period and jitter.

2.14.2 Network Based DDoS Attack Detection Methods

The Radial Basis Function (RBF) method was used by both (Karimazad & Faraahi, 2011) and (Bhuvan et al., 2013). The method could detect DDoS attacks in an efficient way. The RBF method can be applied to edge routers of victim networks. Vectors with seven features are used to activate an RBF neural network at each time window. The RBF neural network is applied to classify data to normal and attack categories. If the incoming traffic is recognized as attack traffic, the source IP addresses of the attack packets are sent to the filtering module and the attack alarm module for further action, and if the traffic is normal, they will be sent to the destination. The RBF neural network method can be performed as an off-line process, but it is used in real time to detect attacks faster.

The honeypot detection technique was first introduced by D.J. Besnstein (Naik, 2015). Besnstein introduced this schema for the Linux kernel patch for version number 2.0.29. (Naik, 2015) used honeypots to detect the DDoS attack. Honeypot detection is still used to direct back a specific node which is a SYN cookie that comprises all the SYN messages. Through using this schema, all the nodes will remain motivated to direct all nodes to the receiver and later the schema will remove the SYN messages from the receiver end. However, the receiver end determines the individual reply to the sender when ACK is sent by a sender laterally with a SYN cookie. This is to stretch a honey node which supports to assign a small retention of data assembly that will ultimately activate an alert when some SYN messages reside in the data structure.

The flooding SYN DDoS attack is a network attacks that renders the information system unavailable. This kind of attack becomes dangerous and more difficult to prevent. In this scenario the attackers try to send flood SYN packets with the spoof source. The author has proposed new method called Packet Identification Anomaly Detection (PIDAD) (Thang & Nguyen, 2016) and it is used to defend against DDoS Attacks. This method is based on abnormal information in the identification field in the IP Header when observing the set of packets received in the victim system.

To detect the DDoS attack on Network Abnormal Behavior in Big Data Environment. The author (Chen et al., 2019) introduce this effective method. This particular method is based on the characteristics of flood attack, the method filters the network flows to leave only the 'many-to-one' network flows to reduce the interference from normal network flows and improve the detection accuracy. The process will define the Network Abnormal Feature Value (NAFV) to reflect the state changes of the old and new IP address of 'many-to-one' network flows. Finally, the NAFV real-time series is built to identify the abnormal network flow states caused by DDoS attacks. (Chen et al., 2019) compare the experiment with the existing methods. This method produces higher detection rate and lower false alarm rate.

Data regulation is intended to reduce the attacker's danger by using, non-honeynet schemes by learning as much as possible about the method. Most of the time the attacker has no knowledge or less technical knowledge. However, data control on honeynet is divided into two different technologies – Network Intrusion Protection System (NIPS) and Connection Counting. First, NIPS strategies review the traffic looking for identified signatures of alerts and exploits once an interruption is noticed. The second technology is Connection Counting, normally used to limit the number of out bound connections a honeypot can pledge (Wang

et al., 2010). In addition, the NIPS are used to drop, will block, alert, prevent or avoid the connection. The IP tables can be organized to deliver connections with limited ability in the honey wall. Moreover, NIPS is used to block and identify known threats by packet examination or inspection.

Author (Sharma & Mukherjee, 2012) propose a feature vitality-based reduction method to recognize reduced important input features in paper intrusion detection using a Naive Bayes Classifier with feature reduction. This method focusses on feature selection or dimensionality reduction and evaluates NSL KDD datasets using the data mining algorithm Naive Bayes Classifier to detect four attack categories namely, probe, DoS, U2R and R2L. Four standard feature selection methods - correlation-based feature selection, information gain, gain ration and the proposed system have been used to apply feature reduction. The author performs comparison with the result of the Naive Bayes classifier model and the feature selection methods and proves that the proposed system is good for network intrusion detection.

Another potential method proposed by author (Fragkiadakis et al., 2015), is based on anomaly-based intrusion detection to detect jamming attacks in a network. The author compares a local algorithm with a collaborative detection algorithm. The local algorithm evaluates based on the Signal-to-Interference-Plus-Noise Ratio (SINR) by executing independently in all monitors. It falls into two categories, simple threshold algorithm and custom change point detection algorithm that have been applied to different metrics of SINR: average, minimum, maximum-minimum-minimum SINR. The collaborative detection algorithm combines the output of the local algorithm, to form a distributed, collaborative intrusion detection system. The paper used the Dempster-Shafer theory of evidence

(Fragkiadakis et al., 2015) as a fusion algorithm, because it does not require any prior knowledge of the system, to make it suitable for anomaly detection, for improving the performance of local algorithms. The performance of both the algorithms is evaluated in terms of detection probability, false alarm rate and its robustness to different threshold values.

Author (Van, Thinh & Sach, 2017) also proposed a similar method called Anomaly Based Network Intrusion Detection System (A-NIDS) to detect a variety of attacks. The paper discussed different approaches to A-NIDS and its pros and cons and performed an analysis on different platforms of A-NIDS based on monitored data that is associated with audit, tracing and forensic capabilities. The authors discussed various open issues and challenges for the anomaly-based detection of unknown attacks and different currently available DDoS systems and platforms. So, this work provides a significant initial point for addressing Research and Development (R&D) in the field of DDoS.

2.14.3 Cloud Based DDoS Attack Detection Methods

The current developments in Software-Defined Networking (SDN) are constructed in the cloud and leads us to innovative probabilities to distinguish the DDoS attack in cloud computing settings (Yan et al., 2015). On one hand, the abilities of SDN, including software-based traffic analysis, centralized control, global view of the network, dynamic updating of forwarding rules, make it easier to detect and react to DDoS attacks. Author (Yan et al., 2015) mention that the relationship between SDN and DDoS attacks has not been well addressed in previous works. The author discussed some understanding of how to make full use of SDN's advantages to defeat DDoS attacks in cloud computing environments and how to prevent SDN itself from becoming a victim of DDoS attacks.

The Ensemble Based Multi-Filter Feature Selection method (Osanaiye et al., 2016) sets out to detect DDoS in cloud computing environments. The proposed method combines the output of 4 filter approaches to attain the best choice which will then evaluate the method with an intrusion detection benchmark dataset and a decision tree classifier. The finding shows that the projected technique can successfully decrease the number of features from 41 to 13 and has a high detection rate. The classification accuracy and detection rate are reasonably good compared to other classification techniques. This particular method is used in cloud computing networks.

The trilateral trust-based defence mechanism against DDoS attacks in cloud computing environment (Iyengar & Ganapathy, 2015) is the proposed "Trilateral Trust mechanism" which helps in detecting different kinds of attack groups at different points of time. The direct trust-based defence mechanism is used for segregating legitimate attack groups from the huge number of incoming requestors. It is a hybrid mechanism of trust that follows the zero-trust approach initially and eventually supports both Mutual trust and Momentary trust. This combinatorial trust mechanism helps in detecting almost all kinds of overload conditions at a cautionary period. Detecting the high rate of attack at an earlier moment of time could reduce the traffic impact on the data centre. The proposed results proved that the mechanism proposed is deployable at data centres for resource protection.

Hybrid Intrusion Detection System (H-IDS) is proposed by (Cepheli et al., 2016) to detect DDoS attacks. To enhance the overall detection accuracy, the authors combined anomaly-based methods and signature-based detection methods. The method applies two distinct datasets to the proposed system in order to test the detection performance of H-IDS and conclude that the proposed hybrid system gives better results than the systems based on non-

hybrid detection. However, 2 papers (Modi et al., 2012) and (Navaz, Sangeetha & Prabhadevi, 2013) have used Anomaly-Based methods to detect DDoS attacks but the result is not really effective to detect DDoS attacks compared to H-IDS and the attack detection accuracy is also lower than H-IDS detection.

Detection of malicious users using the "Group Testing" technique, prevents some legal systems from getting compromised (Thai et al., 2008). The technique tracks the handler or agent behaviour and allows the system to understand better how to defend against future DDoS installation attacks. Their scheme had several drawbacks. First, the method assumes that the attack must be detectable using signature-based detection tools. If not, the packet is forwarded to the destination in operational networks.

The detection and prevention of DDoS attacks remains a most important concern for users, businesses, academics and researchers (Rawal, Ramcharan & Tsetse, 2013). Innovative measures are established to avoid or alleviate DDoS attacks, yet attackers are constantly developing innovative techniques in turn to counter these new measures. As a response to DDoS, the Augmented Split-Protocol (ASP) (Rawal, Ramcharan & Tsetse, 2013) was introduced. The travelling nature and role change over different servers in a split-protocol architecture will avoid a bottle neck on the server side. It also offers the exclusive ability to prevent the server capacity from being overloaded and compromised by DDoS attacks. The most popular methods are open source signature-based detection (Zeadally et al., 2012). Early botnets were organized in a centralized or structured manner with each bot communicating directly, or through the covert station, with the knowledge and control node. Botnets will receive commands from the control node. Botnets are more sophisticated,

creating a hierarchy of command and control servers to make it harder to track down the central command and control server.

Author (Sahi et al., 2017) discussed DDoS attack detection in cloud environments. The DDoS attack remains the most predominant cybercrime attacks for data theft. In addition, DDoS TCP flood attacks will consume the cloud's bandwidth, consume most of the resources, and also harms or damages a whole cloud development in a short time. Besides that, the appropriate prevention and detection of such attacks is very important in cloud developments and it is consequently dynamic, particularly aimed at eHealth clouds. Furthermore, the innovative classifier systems for preventing and detecting DDoS TCP flood attacks in public clouds are very difficult. Detection schema propose an answer to safeguarding records through categorizing the incoming packets and making a decision based on the classification results. Through the detection stage, it will determine and identify whether a packet is ordinary or initiated from the attacker. Through the anticipation stage, all the packets which remain secret as being malicious will be denied entrance to the cloud service and the system will backlist the IP address. The algorithm of the approach is linked using the dissimilar classifiers of the least squared support vector machine Naïve Bayes and the multilayer perceptron.

2.14.4 Cluster based DDoS Attack Detection Methods

Clustering is the process of grouping similar data or network traces which were identified as malicious. By grouping the network traces into different groups, the problem of DDoS attack detection can be approached efficiently (Zhong, & Yue, 2010). Once the network traces are grouped, then the newly captured packet features can be classified by using some similarity measures. In the connection phase, the boot establishes a connection back to a command and

control server in a centralized architecture. A similar technique is used by (Chaabouni et al., 2019) to demonstrate that highly efficient and accurate signature-based classifiers can be constructed by using essential network features and machine learning techniques to detect DoS attacks at the edge controllers.

By nature, the Internet is public, connected, distributed, open, and dynamic. The extraordinary growth of computing devices, connectivity speeds, and some applications running on networked systems poses a risk to the Internet. Malicious usage, attacks, in addition to sabotage, are on the increase as more and more computer devices are placed into use. Connecting systems in sequence to a network such as the Internet in addition to public phone systems further magnifies the potential for contact with an assortment of attack channels. These attacks take advantage of the flaws or omissions that exist within the various information systems and software that run on many hosts in the network.

The ANN based Scheme (Gupta, Joshi & Misra, 2012) aims to predict the number of zombies involved in a DDoS Attack and needs to accept an encoding method. There are many existing IP back track schemes using different encoding methods. In this method, the researchers choose the Advanced Marking Scheme (AMS) (Gupta, Joshi & Misra, 2012). When the victim begins to rebuild the attack graph, it does not need to recreate such a long path. The simulation shows that as long as most of the infected edges within ten hops are reconstructed, the filtering scheme will achieve its goal.

Regardless of the countless attempts to protect wireless sensor networks (WSN), (Elhoseny et al., 2016) suggested a clustering-based data routing scheme using the Elliptic Curve Cryptography (ECC) with homomorphic encryption methods. A genetic algorithm is applied

in this method for optimizing the network structure and its ranges. Depending on the ranges, those nodes inside the ranges are formed as one group. To provide high security in the network, the public key is exchanged in different sizes. (Dahane et al., 2015) also proposed a clustering algorithm to solve the security issues in clustering. (Dahane et al., 2015) propose a distributed and safe weighted clustering algorithm, which is an extension of the ES-WCA algorithm. The main goal is to find some routing problems and attacks on the network. A safe and a stable CH was elected based on the five metrics, mobility, residual energy, connectivity, distance of the nodes and balanced level of the neighbour. Using the metrics, the proposed algorithm chooses the robust CH with the highest value to monitor and maintain the cluster locally. As a result of monitoring by CH, the algorithm can also detect the presence of intruders in the network. The algorithm evaluates its performance by simulation in mercury and finds that there is minimal consumption of energy in the entire network, thereby it increases the lifetime of the network and thus provides a stable and reliable environment.

A greedy algorithm is proposed by Andrysiak, Saganowski & Chorań (2013) detects DDoS attacks and network anomalies. The algorithm is used to find a best solution for anomaly detection by means of iterative procedure. It performs by using a Matching Pursuit (MP) algorithm and an Orthogonal Matching Pursuit (OMP) algorithm in a cluster-based representation. The aim of the MP algorithm is to achieve a fair input signal by sequential selection of best atoms, which is the residual of signal for each of the iterations. The algorithm terminates when the residual is less than the acceptable limit. OMP is an improvement of MP where the selected atom is to be orthogonal for each of the iterations, and finally the algorithm ends when the requirement is satisfied. Furthermore, a new ID KSVD algorithm has been proposed for anomaly detection. The algorithms are evaluated in

a tree-based structure, and Overall Detection rate (ODR) is calculated for detecting DDoS attacks using Detection Rate (DR) and False Positive Rate (FPR) parameters. It has experimentally proved the efficiency of the Greedy system in detecting DDoS attacks and network anomaly detection attacks.

Defense mechanisms countering DDoS attacks in the network at the DoS attack program have been in existence for several years. The sources of single basis attacks are countered with no trouble by lots of available protection mechanisms. These can be de-activated with no problems using better tracking techniques (Gibbs, 2014). With the considerable growth of the Internet, progressively more vulnerable systems have become available to attackers. Attackers can employ these vulnerable hosts to launch an attack. For instance, cross-plane correlation involves cross-checking clusters in both planes that show similar activities between nodes that share communication patterns. A score is computed indicating the likelihood of botnet membership.

Author (Nguyen, Lin & Hwang, 2018) developed a traditional source-based anti-DDoS technique based on consideration of the traffic model for secure networks, but it is not extremely effective when used for mobile networks. The authors propose an innovative DDoS defense architecture by using a hybrid detection method that associates with network-based and source-based filtering mechanisms. Presently, mobile edge computing remains accessible to nearness of cellular base stations to address a wide range of use cases that need edge computing such as real-time on-demand services in the IoT ecosystem. Consequently, the authors proposed a design for source-based component related to architecture to be combined inside servers instead of adjusting present routing protocols. Furthermore, the main aim of this study is to alleviate the network footprint and attack traffic by riddling or filtering DDoS flooding attacks near to sources as much as possible.

2.14.5 DoS and DDoS attack detection methods in MANET

Dhaka, Nandal & Dhaka (2015) propose a scheme to identify malicious node at MAC layer while accessing the channel in the paper's Gray and Black hole identification using control packets in MANET (Schweitzer et al., 2016). The author establishes two control packets, Response Sequence Packet (Rseq) and Code Sequence Packet (Cseq) in the existing AODV routing protocol. These packets are broadcast in the AODV-MAC at the time to access the channel and it is exchanged between the intermediate node and the neighbour node to maintain a secure connection in the network. If these packets are equivalent with the neighbour, then the connection between the neighbour and the intermediate is accepted, otherwise it is discarded and broadcasted that the node is malicious. The presence of malicious nodes happens at the initial stage itself and they are removed immediately without delay or further processing.

The Author (Balan et al., 2015) used fuzzy based detection techniques in MANET to solve black hole and gray whole attacks. The system is strong enough to detect both black hole and gray whole attacks via an efficient node blocking mechanism. The proposed system first identifies the type of attack and informs to the next fuzzy implementation module. The fuzzy logic is implemented by using the measures of number of packets dropped against the threshold value and the relational matrix is calculated by using various parameters. Using the value of the matrix, fuzzy estimation is performed by calculating the matrix value against threshold value, number of packets formed, and number of packets dropped. At the end Intrusion detection gets the input from the fuzzy technique, classifies the type of attacks and identifies the malicious node. After detection of malicious node, the system changes the direction of packet flow by using the AODV protocol to provide a secure communication. (Su, 2011) also discusses the detection methods for the black hole attack in MANET

environments. The method is called Anti-Black hole Mechanism. It uses AODV as a routing protocol to evaluate DDoS in MANET. This method estimates the suspicious value of a node based on abnormality between RREQ and RREP transmitted from the node. If the suspicious value exceeds the threshold value, a block message is initiated by a node, generated by the nearby DDoS and broadcast to the network to isolate the malicious node. The block message contains the information about the node that issued the block message, the malicious node itself and the time of identification. On receiving the block message, the node isolates the malicious node as an attack and enters it on the blacklist. The author implemented the system using NS2 and validated the effect of DDoS by blocking the malicious node. He showed that the system effectively detects malicious nodes and successfully reduces the packet loss rate.

According to (Xiang et al., 2011) there are many DDoS attack detection methods in MANET, but they did not work well because of their dynamic nature. Besides that, this author (Xiang et al., 2011) introduces a Security-Aware Routing protocol (SAODV) that will sort out available nodes on unrelated or dissimilar security levels. Two types of nodes are used in this paper: the first are Remote Protection Nodes (RPN) and the second are Local Protection Nodes (LPN). Lower level nodes become the LPN and defend high or difficult level nodes to reach their destination securely, whereas the beginning node on the source becomes the RPN to detect hateful or malicious packets and it successfully reduces the packet loss rate.

As MANETS are highly vulnerable to various attacks, (Kaur, Toor & Saluja, 2014) propose a clustering reputation mechanism to identify flooding attacks in MANETs. Flooding attack is one of the most dangerous attacks, where an intruder overloads the network to misuse the bandwidth consumption and resources of the network. The authors implement the

mechanism in military applications, where a group mobility model is followed, to group the nodes in clusters. An AODV protocol was modified and reputation has been calculated to analyze the behaviour of the node. Based on the calculated value, malicious nodes can be identified. No malicious node can flood the packet at a high rate, if the reported value is less. Various performance metrics have been evaluated through simulation to detect the presence of flooding attacks and minimize the overhead in the network. (S'nchez & García, 2012) also proposed a similar method.

The Enhanced Adaptive Acknowledgement (EAACK) method was introduced by (Shakshuki, Kang & Sheltami, 2013) to overcome the security issues in MANETs. The proposed scheme solves the problem of watchdogs to improve the performance of the network in the presence of intruders. EAACK is an enhancement of the previous AACK algorithm and it is extended by using a digital signature to prevent attackers from modifying acknowledgements. It consists of three parts: ACK, Secure-ACK (S-ACK), and Misbehaviour Report Authentication (MRA). ACK acknowledgement packets were sent between source and receiver if there is no misbehaving intermediate node between them. Otherwise, it switches to S-ACK by sending a secure acknowledgement packet to detect the misbehaving node. MRA is used to detect malicious nodes in spite of the presence of a false misbehaviour report. All the acknowledgement packets should be digitally signed by the sender and should be verified by the receiver. The author simulates and compares the performance with Watchdog, TWO-ACK and EAACK in three cases, namely, receiver collision, limited transmission power, and false misbehaviour reports and provides a positive result in the detection of attacks.

To improve attack detection, (Deny & Sivasankari, 2011) proposed a distributed method of emerging authentication and intrusion detection to improve security in MANETs. Since MANET has been popular in military applications, it is highly desirable to provide a secure and reliable communication in such environments. Thereafter, two paired classes of security approaches are needed for MANETs in a hostile environment: a prevention-based approach and a detection-based approach. Authentication is used for the prevention-based approach and intrusion detection is used for the detection-based approach. Biometric technology has been used for authentication and it is the first line of defense, but, for a high security mechanism we need a second line of defense, therefore, DDoS is used to identify the malicious activities in the network. The proposed system uses fingerprint or Iris biometrics to authenticate and activate the nodes and forwards the authenticated message to the entire network. The received nodes reply ACK message to the respective nodes and provide secure communication. The DDoS detects and blocks the intrusion, in its presence. To improve the detection of DDoS, the Dempster-Shafer theory has been used together with sensor fusion, due to more than one node being used at a time. By simulation the author (Deny & Sivasankari, 2011) shows that the proposed system improves the performance of network security.

One of the most serious attacks that affects the normal working of MANETS is the DoS Attack (Doss et al., 2018). A type of DoS attack is the Jellyfish attack, which is relatively firm because of its rummaging behaviour. In addition, the Jellyfish attack is viewed as the most problematic attack to detect and damage the performance of the overall network. To combat Jellyfish attacks in MANETs, a new approach has been proposed, named accurate prevention and detection of jelly fish attack detection (Doss et al., 2018). It is a mixture of Support Vector Machine (SVM) and an authenticated routing-based framework for detecting

attacks. SVM is applied for learning packet forwarding actions. The method selects trusted nodes in the network for performing routing of packets on the basis of the hierarchical trust assessment properties of nodes.

2.15 Conclusion

In conclusion, this chapter has focused on the existing work on the Denial of Service and Distributed Denial of Service attacks. This chapter covered in depth the characteristics of VANET, and challenges of VANET and VANET applications. Besides that, types of attacks were discussed with diagrams. Finally, the author has examined some of the literature about DoS and DDoS attack detection methods in 5 main areas: VANET, MANET, Cloud, network and cluster.

CHAPTER 3: PROBLEM ANALYSIS

3.1 Introduction

This chapter discusses DDoS attacks in VANET. Nevertheless, performance metric comparison for DDoS attack detection methods in VANET are also discussed. Some of the drawbacks and taxonomy of detection methods is also discussed in Section 3.5. Section 3.6 will deliberate on the VANET security publication statistics from 2009 up to 2018.

3.2 DDoS attacks in VANET

DDoS attacks are very dangerous in vehicular communications because the process of the attack is distributed, and the impact is disseminated throughout the network. In this attack, the attacker takes control over other nodes in a network and launches attacks from different locations. DDoS attacks are launched from multiple connected devices that are distributed across the Internet. These multi-person, multi-device barrages are generally harder to deflect, the attack source is more than one, often thousands of, unique IP addresses, mostly due to the sheer volume of devices involved. Unlike single-source DoS attacks, DDoS attacks tend to target the VANET infrastructure in an attempt to saturate it with huge volumes of traffic. In DDoS attacks, the attacker will send a message to victims from different locations and might be using different time slots to send the messages. The attacker may change all time slots and the messages themselves for different nodes. The goal of the attack is to make the network unavailable to victim nodes by bringing the network down.

The VANET, with its latest technology, has been used in many emerging applications. However, the VANET network is prone to various vulnerabilities, degrading the performance of QoS. Therefore, this chapter deals with various detection techniques and

algorithms created by many researchers. VANET is presently considered as one of the best-performing technologies for road accident avoidance and works by permitting the V2V to share information related to the traffic. As we know, VANET is also used for infotainment applications and traffic management (Hasrouny, Samhat, Bassil & Laouiti, 2017). The most important characteristic of VANET is scalability and flexibility which is essential to understand the arrangement of VANET services competently.

Owing to fast moving vehicles and the dynamic exchange of information, vehicle nodes are relatively high speed, therefore maintaining and finding routes is a very challenging task in vehicular networks. In the vehicular network, data wandering from sender to destination will suffer from huge packet delays and packet loss due to cramming in between nodes. Besides that, reliable communication in VANET is vital to develop reliable and functional traffic safety and competence applications. Naturally, applications on VANET require video, data and voice transmission over vehicle-to-vehicle communication. Nevertheless, the Voice over IP (VoIP) may offer good facilities through VANET's platform. It will cover a lot of applications, ranging from comfort related services to safety services (Mershad & Artail, 2012).

VANET is increasing gradually in use as it improves the safety of passengers. As VANET is used in the open wireless medium, it attracts numerous possible attacks. The adaptable nature of networks attracts problems associated with security and traffic safety. Network accessibility has been threatened by DDoS attacks. Wherever attacks have initiated the network to breakdown, confidence in the network might not be good if a life-critical message is changed by criminals before it is established by the intended receiver and consequently, it is significant to sustain the network's accessibility and to increase confidence in the VANET

infrastructure, mainly for safety-critical requests to be beneficial. The objective of the offender was to initiate problems for authorized users, and as a consequence, services are not accessible, leading to a DDoS attack (Mershad & Artail, 2012) (TamilSelvan & Rajendiran, 2013).

3.2.1 General Attack Scenario and Limitations

- All the nodes in a VANET (vehicle nodes and the RSU) act as both transmitters and receivers.
- The mobility of vehicles is continuous and very fast, especially on highways.
- Thus, the communication links between each vehicle are just for several milliseconds. The links are established and broken quickly. The result is a rapidly changing topology.
- Predictable Mobility: Vehicles are run on pre-built roads and highways, therefore the motion shape of vehicles can be forecast based on the road layout and topology.
- However, there could be some uncertainty in the movement of vehicles depending upon the layout of the road, the traffic density, structure of lanes and of course the behaviour of the drivers.
- High Speed: in VANETs the node moves very quickly compared to MANETs
- Variable Node Density: in the VANET, the number of nodes can be very busy in remote highways and normal roads.
- Equally, in certain areas, the traffic conditions may be minimal during the midnight hours and traffic will be heavy during busy office hours. Therefore, any protocol designed should take into consideration both scenarios.

3.3 Existing and Common Attack Detection Mechanisms in VANET Networks

This section is basically analyses on existing DDoS attack methods in VANET and also to find the research gap. Moreover, to identify weaknesses from the paper and direction to the solution. This is to show the results from the existing research paper, so that we able to see the improvement in the development models result. Nevertheless, security is one of the main problems in VANET networks, owing to the mobile nature of the vehicles. In an attack situation, the behaviour of the attacker will change and broadcast vast amounts of false data in VANET networks. To solve this issue, the author (Pathre, Agrawal & Jain, 2013) proposed a novel traffic congestion detection and removal schema against DDoS attacks. Another solution was suggested by Biasi, Vieira & Loureiro (2018) for flooding attack detection using the SDM. The issue with Sentinel is that it will be vulnerable from attack if the attacker changes the method of attack from constant traffic flow signal flooding to variable types of traffic signal flooding. If the attacker is able to achieve that, the detection method will probably not hold up. The system will only register the attack as changes in traffic and adapt to the changes with a different traffic flow. The outcome of the simulation result for mitigation rates is 78% and the PDR value is 92%. Nonetheless, the algorithm is able to mitigate the attack flow under dissimilar constraints or parameters. The detection time is increasing, and the system cannot increase the PDR value.

In most situations in vehicular networks, sensitive information will be transmitted. Sometimes, it will affect important safety decisions in vehicle-to-vehicle communication. In vehicular communications the network faces numerous types of security attacks. Nonetheless, these are DoS and DDoS attacks. The both attacks are rapidly increasing problems. Biswas, Mišić & Mišić (2012) proposed a mitigation technique that uses synchronization-based DDoS attacks on vehicular communications to avoid DDoS attacks.

Hussein, Elhajj, Chehab & Kayssi (2017) proposed three-way integration among 5G, VANET, and SDN for a strong VANET security design approach. This method is for a resilient VANET security design approach, which results in good stability in network performance, security features and mobility. This method shows how to trace back the source of the attack if any attack happens in the vehicular network. The outcome of this method is to minimalize the configuration and maintain low overhead.

More than twenty-five papers discuss security in vehicular communications. Here, the latest articles that deal with security in vehicular communications will be discussed. The first method is P-Persistent scheme (Alwakeel & Prasetijo, 2014) that is designed to decrease message cramming and enhance the performance of message distribution in VANETs. The second method uses ticket-based authentication schema (Chikhaoui et al., 2018). This method uses a temporary ticket for the vehicles to communicate with each other while protecting their privacy and security. To send the trustworthiness message among the vehicles, the authors proposed an effective message trustworthiness scheme to broadcast reliable incidence messages in a timely manner in vehicle-to-vehicle communication. The third method is novel cross layered design CLARR (Cross Layer Autonomous Route Recovery) (Shafi et al., 2018), which was designed for effective multimedia message distribution. It is highly challenging to achieve high data transfer rates in a vehicular network, because of frequent topology changes and frequent link breakage.

To overcome this issue, the researcher (Ahmad et al., 2018), used a cross layered design CLARR, which will take the most stable and the shortest paths against inherent actions in the network like random topology changes and frequent link breakage. In this method there are two mechanisms: the first is to include a new field format to calculate the highest link

lifetime. The second is to request to provide vehicles with possible hops to destination using intermediate nodes, thus reducing the percentage of route error extensively. The fourth method is the Chain-based data dissemination in vehicular ad-hoc networks (VANETs), which is used to improve the throughput of service packets by maintaining acceptable probability of successfully received safety packets (Ahmad et al., 2018). On top of that, the essential dynamicity can remain realized once the vehicle density is low in rural areas, and a portion of the assigned time has passed for safety packets to transmit data packets on SCHs (Service Channels) without losing broadcasted safety packets during CCH (Control Channel) intervals.

In this thesis, the literature on DDoS attacks in VANET was analyzed. According to the performance metrics analysis results, most of the papers focus on the Packet Delivery Ratio (PDR). Here, the outcomes from the 6 most relevant methods will be shown (Bansal et al., 2015), (de Biasi et al., 2018), (Vipin & Chhillar, 2018) (Shabbir et al., 2016), (Bansal & Pawar, 2015) (Kaur & Mahajan, 2015).

The PDR analysis result is shown in Figure 3.1. The values according to the PDR percentage and 80 nodes have been calculated so that we can see the differences in PDR. The second performance metric is attack detection time. The detection time is important so that other nodes can identify the attack as fast as possible so that a particular node will avoid sending the message to the attacked node. Most authors did not reveal accurate times to detect attacks in their papers. Out of 10 methods, only 2 Bansal, Sharma & Prakash (2015) and Shabbir, Khan, Khan & Saqib (2016) showed the attack detection time in their papers. One paper (Bansal & Pawar, 2015) mentioned that attacks could be detected within 1 second. The comparison of result on detection time is shown in the Figure 3.2. In the scenario, when the

number on nodes in the network is zero, all the existing methods and proposed method are not able to perform the attack detection. The existing methods results shown in the Figure 3.2. Moreover, I have shown the proposed models result in the simulation results section in the chapter 5. The graph are showed zero when there is no nodes. Specially for attack detection time and attack detection rate.

The third network performance metric is throughput. The throughput is the total data stimulated effectively from one place to another in a specified time period, and it is calculated in megabits per second (Mbps) or in bits per second (bps). Throughput is a measure of network performance. However, only two papers (Vipin & Chhillar, 2018) and (Kaur & Mahajan, 2015) discussed throughput, and Figure 3.3 shows throughput in different methods.

The fourth performance metric is Packet Drop Ratio. Out of 10 methods only 3 (Vipin & Chhillar, 2018) (Biswas et al., 2012) and (Kaur & Mahajan, 2015) discussed packet drop ratio. Figure 3.4 compares the Packet Drop Ratios for different methods. Such packet loss is also triggered by faults in data transmission, typically network congestion or across wireless networks. Packet loss is measured as a percentage of packets lost against packets sent.

The fifth performance metric is Attack Detection Rate. Only three paper discusses this (de Biasi et al., 2018). One more potential performance metric is end-to-end delay. Out of 10 papers, only one discussed the End to End Delay. The end to end delay denotes the time engaged for a data packet to be transmitted across a network from source to end point or destination. Table 3.1 shows the comparison of the performance metrics. According to the analysis, the packet delivery ratio is really important because the packet should be delivered

to its destination on time without any delay specially for safety-critical applications. At the same time, attack detection time also plays an important role because if an attack is happening then the packet or node will be delayed in reaching the other vehicle or RSU. Life critical information should be delivered on time; if it is not on time, then it is meaningless. None of the 12 existing VANET DDoS attack detection methods discussed the false classification ratio and routing overhead performance metrics.

All the results for Figure 3.1, Figure 3.2, Figure 3.3 and Figure 3.4 are collected from the existing research paper (Kaur & Mahajan, 2015), (de Biasi, Vieira & Loureiro, 2018), (Vipin & Chhillar, 2018), (Bansal, Sharma & Prakash, 2015), (Sahare & Malik, 2014), (Pathre, Agrawal & Jain, 2013), Pavan , Sarma & Reddy, 2019), (Poongodi et al., 2019).

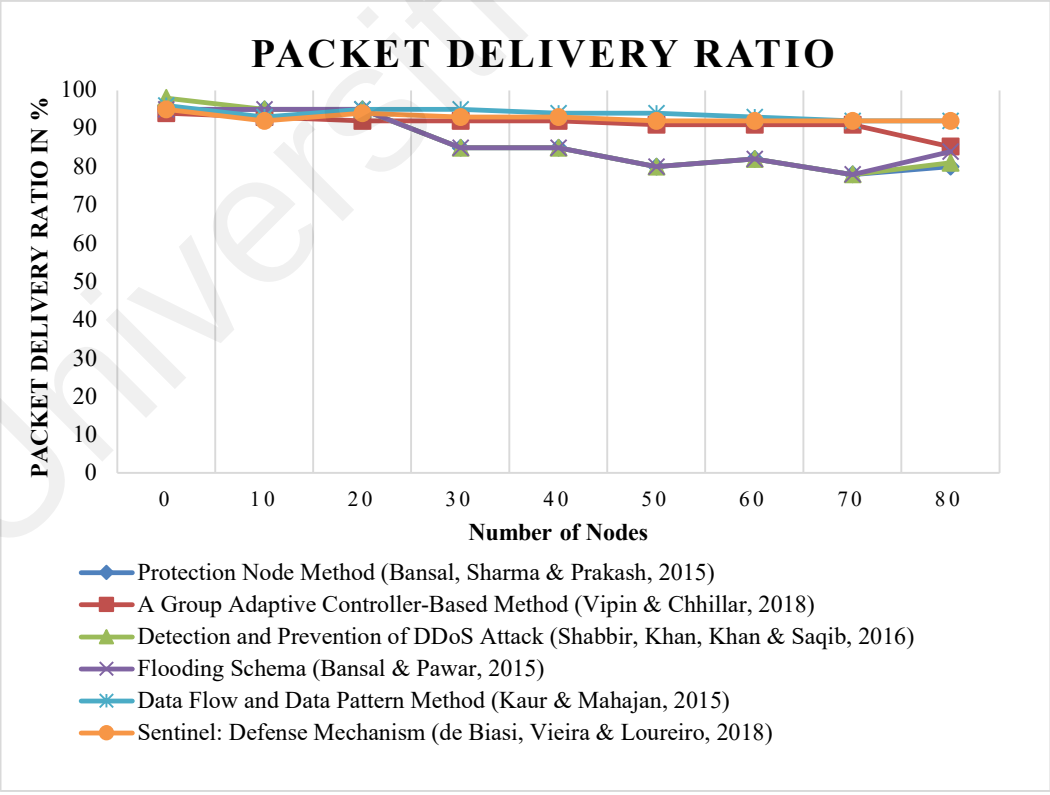

Figure 3.1: Comparison of Results of Packet Delivery Ratio (PDR)

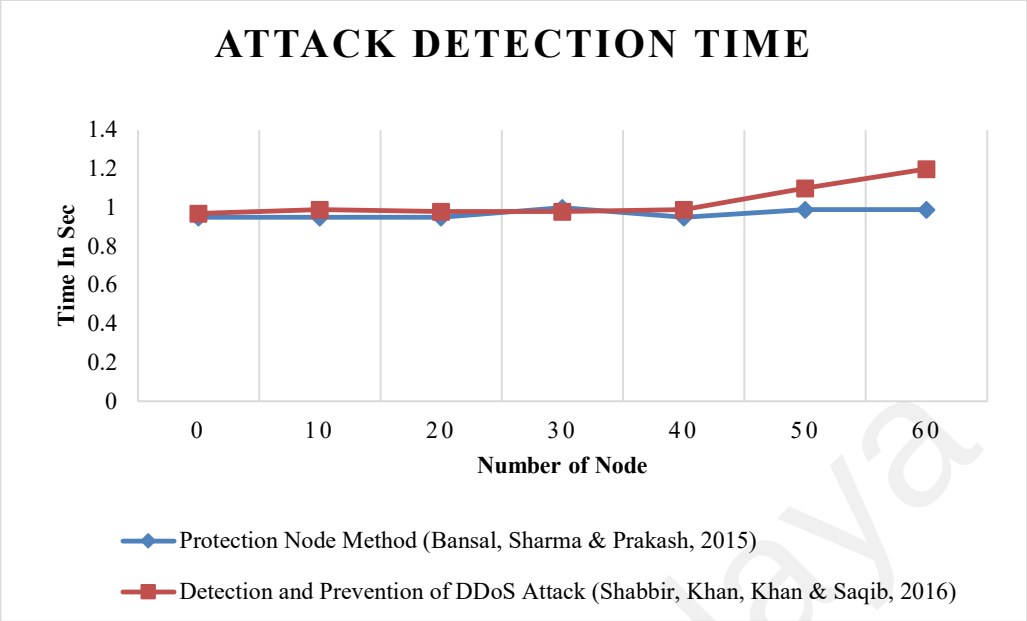

Figure 3.2: Comparison of Results of Attack Detection Time

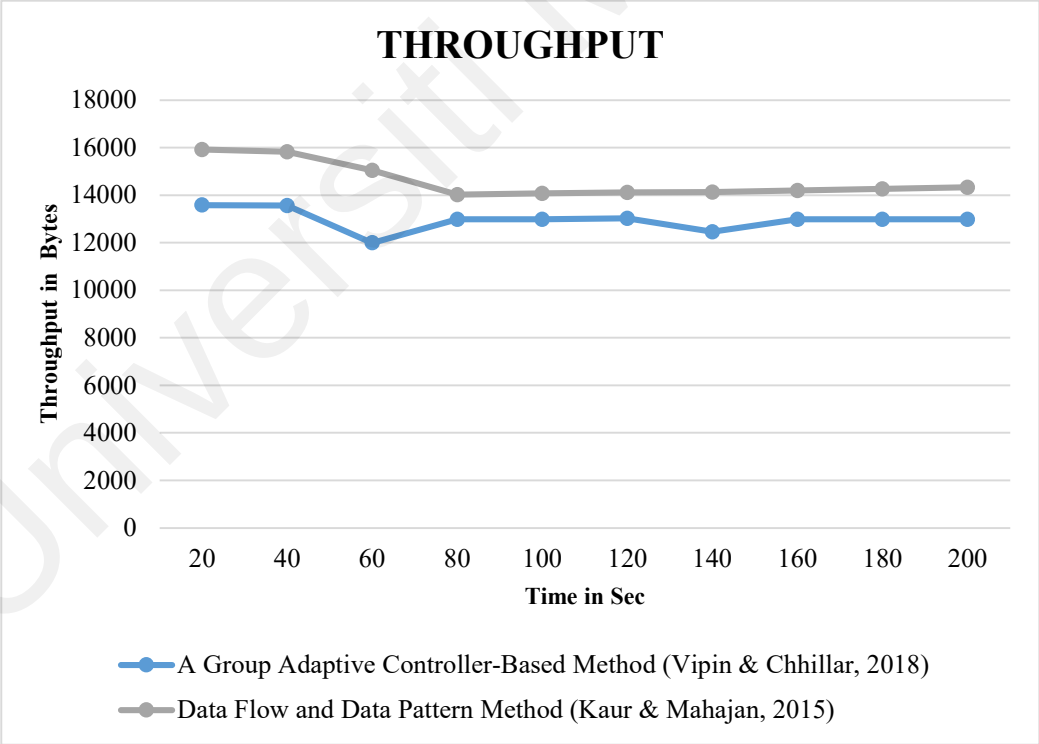

Figure 3.3: Comparison Results of Throughput

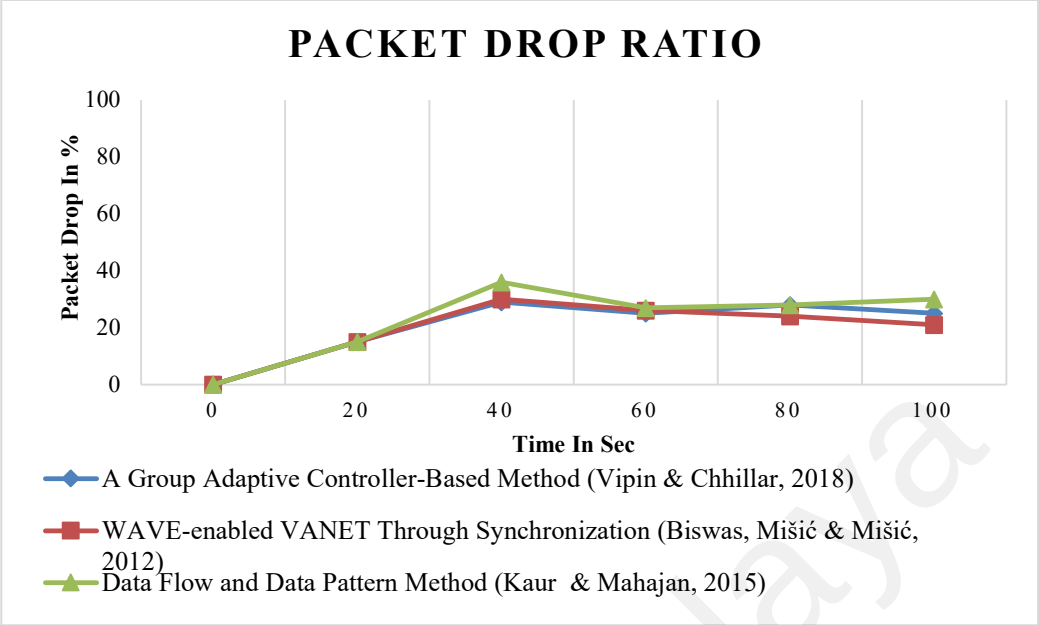

Figure 3.4: Comparison of Results on Packet Drop Ratio

Table 3.1: Performance Metric Comparison for DDoS Attack Detection Methods in VANET

Name	Attack Detection Time	Attack Detection Rate	Throug-hput	End to End Delay	Packet Delivery Ratio	Packet Drop
A Novel approach for Detection of Distributed Denial of Service attack in VANET (Bansal, Sharma & Prakash, 2015)	√	X	X	X	√	X
Sentinel: Defense Mechanism against DDoS Flooding Attack in Software Defined Vehicular Network (SDM) (de Biasi, Vieira & Loureiro, 2018)	X	√	X	X	√	X
The DDOS Attack Detection and Prevention in VANET by Group Controlled Analysis Model (GAC) (Vipin & Chhillar, 2018)	X	X	√	X	√	√

An Approach for Detection of Attack in VANET (Sahare & Malik, 2014)	X	X	X	X	X	X
A Novel Defense Scheme against DDOS Attack in VANET (Pathre, Agrawal & Jain, 2013)	X	X	X	X	X	X
Detection and Prevention of Distributed Denial of Service Attacks in VANETs (Shabbir, Khan, Khan & Saqib, 2016)	√	X	X	X	√	X
DDoS Attack on WAVE-enabled VANET Through Synchronization (Biswas, Mišić & Mišić, 2012)	X	X	X	X	X	√
Identification of Malicious Vehicle in VANET Environment from DDoS Attack (Ayonija & Jain, 2013)	X	X	X	X	X	X
Reducing Impact of Flooding In VANETs Due To Distributed Denial of Service Attacks (Bansal & Pawar, 2015)	X	X	X	X	√	X
A Novel Security Approach for Data Flow and Data Pattern Analysis to Mitigate DDOS Attacks in VANETs (DF) (Kaur & Mahajan, 2015)	X	X	√	√	√	√
Classification of DDOS Attacks in VANETs based on Distributive Collaborative Framework (Pavan , Sarma & Reddy, 2019)	√	√	X	X	X	X
DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET (Poongodi et al., 2019)	X	√	X	√	X	√

3.4 Drawbacks of the existing DDoS Attack Detection Methods

The investigations and studies of existing DDoS attack detection methods in VANET show some drawbacks in current methods. Table 3.2 shows the drawback of the existing DDoS attack detection methods. (Bansal et al., 2015) introduce the protection node concept to detect DDoS attacks in vehicular communication. The Local Protection Node (LPN) is selected from the hierarchical architecture. The PDR value and the threshold value have been compared, and when these two values become equal a Monitor Mode message is transmitted by LPN to other vehicles in the network for the purpose of sensing. Any vehicle that injects large number of false packets will be detected as an attacker and thus packets from the bad node will be discarded. The research is explained well, and the concept is efficient. The method focuses on PDR, threshold value and detection time. The algorithm is unable to increase the PDR and the detection time was less than two seconds.

(Vipin & Chhillar, 2018) introduce the Group Adaptive Controller-Based method, which achieves almost the same results. Both methods use 50 nodes to test. The Group Adaptive Controller-Based method produces 12987 packets throughput in 200Sec. But the protection node approach did not mention throughput. (Sahare & Malik, 2014) introduced the Fuzzy Logic Detector (FLD). This FLD method did not produce any results, but the author did discuss the algorithm. The FLD method did not achieve attack detection and provided no VANET traffic analysis. The author only shows the DDoS detection packet and did not justify the time of the attack detection. (Ayonija et al., 2013) introduced a new mechanism to detect malicious vehicles in the network, but this method did not produce any results.

Nonetheless, the WAVE-enabled VANET Through Synchronization (Shabbir et al., 2016), (Biswas et al., 2012), Flooding Schema (Bansal & Pawar, 2015) and the Novel Security

Approach for Data Flow and Data Pattern Analysis to Mitigate DDoS attack in VANETs (Kaur & Mahajan, 2015) used less than 30 nodes for simulation. The proposed model result has been obtained on the basis of network load, throughput and packet delivery ratio. The experimental results have proved the efficiency of the proposed model in comparison with the existing models. For the WAVE-enabled VANET Through Synchronization method, (Biswas et al., 2012) analyze the prospect of a synchronization-based DDoS attack on vehicular communications and proposed mitigation techniques to avoid such an attack. In the flooding schema, the authors did not identify the safety packet node and non-safety packet node. The method only focuses on request messages and did not use any live exchange messages. All the existing VANET DDoS detection methods that we have discussed did not classify the packet according to the safety message packet/node and non-safety message packet/node. All the existing VANET DDoS detection methods did not identify the attack severity levels after detection. If an algorithm identifies the attack severity level then in future if similar patterns of attack packets enter the VANET network, then the packet will be terminated earlier.

Table 3.2: Drawback of the existing DDoS Attack Detection Methods

Title	Approach/Method	Drawback
A Novel approach for Detection of Distributed Denial of Service attack in VANET (Bansal, Sharma & Prakash, 2015)	The algorithm uses the concept of "protection node"	- The approach focuses on PDR, threshold value and detection time. - The system cannot increase the packet-delivery ratio. - Focusing with 3 metrics - Detection time less than two seconds.
Sentinel: Defense Mechanism against DDoS Flooding Attack in Software Defined Vehicular Network	Sentinel: Defense Mechanism	- The overall mitigation rate is 78% and PDR value is 92% - The detection time is increasing - Detection time less than one second.

(SDM) (de Biasi et al., 2018)		- The system cannot increase the packet-delivery ratio. - Focusing with 2 metrics
The DDOS Attack Detection and Prevention in VANET by Group Controlled Analysis Model (Vipin & Chhillar, 2018)	A Group Adaptive Controller-Dased Method	- Experiment in small scale (50 nodes) - Focusing on throughput, communication loss, PDR value and other metrics are not mentioned. - Detection time less than one second. - Proposed model: throughput 14325 packets in 200Sec, PDR 85.27% and Communication Loss 0.83% - Focusing with 3 metrics
An Approach for Detection of Attack in VANET (Sahare & Malik, 2014)	Fuzzy logic Detector (FlD)	- The approach did not achieve attack detection and no VANET traffic analysis - The author only shows the DDoS detection packet and did not justify the time of the attack detection happen. - No performance metric is discussed.
A Novel Defense Scheme against DDOS Attack in VANET (Pathre et al., 2013)	Novel traffic congestion detection and removal scheme against DDoS attack	- Author did not reveal anything about the overall throughput and detection time. - If there is an attack some control packets deliver on time which is 37secs. - Focusing with 2 metrics (Control packet analysis and traffic behavior)
Detection and Prevention of Distributed Denial of Service Attacks in VANETs (Shabbir et al., 2016)	Detection and Prevention of Distributed Denial of Service Attacks	- According to this method, the PRD Value is 79%. - According to the author the results of the algorithm are satisfying. But there is still a lot more scope for achieve the maximum efficiency. - Detection time less than one second

		- Author did not reveal anything about the overall throughput. - Focusing with 2 metrics (Detection time & PDR)
DDoS Attack on WAVE-enabled VANET Through Synchronization (Biswas et al., 2012)	WAVE-enabled VANET Through Synchronization	- Effect are going worse when, neither the receivers or sender of periodic broadcasts will be alert of the attack since broadcast. - Focusing with 1 metric (Packet Drop Ratio)
Identification of Malicious Vehicle in VANET Environment from DDoS Attack (Ayonija & Jain, 2013))	Identification of Malicious Vehicle	- Did not provide any method to detect/identify DDoS attack in VANET environment. - No performance metric is discussed.
Reducing Impact of Flooding In VANETs Due To Distributed Denial of Service Attacks (Bansal & Pawar, 2015))	Flooding Schema	- Experiment in small scale (24 nodes) - Focusing with 1 metric (Packet Delivery Ratio) - The author did not identify the safety packet node and non-safety packet node. - Only focusing on request messages and did not use any live exchange messages.
A Novel Security Approach for Data Flow and Data Pattern Analysis to Mitigate DDOS Attacks in VANETs (DF) (Kaur & Mahajan, 2015)	Novel Security Approach for Data Flow and Data Pattern	- Experiment in small scale (15 nodes) - Focusing with 4 metrics (PDR, End to End Delay, Throughput & Packet Drop) - The author only shows the overall throughput and did not justify the time of the attack detection happen. - Did not show the Cluster selection in the algorithm.

3.5 Availability in DDoS Attacks

The availability requirement implies that every node should be capable of sending any information at any time. As most interchanged messages affect road traffic safety, this requirement is critical in this environment. Designed communication protocols and

mechanisms should save as much bandwidth and computational power as possible, while fulfilling these security requirements. It is present on all communication patterns, that is, it affects not only V2V communications, but also V2I.

If the network is not available for communications due to a DDoS attack, then the main goal of the network is pointless. For instance, in an accident, a user will not be able to send information to another vehicle. Alternatively, a user will not be able to download multimedia files from an RSU. DDoS attack is one of the key attacks on the availability of the network. Channel jamming in wireless environments is also part of this attack and the objective of the attacker is to prevent authentic vehicles to access the network services. The attack may jam the whole channel or may create some problems directly or indirectly to utilize the resources of the networks and the system is no longer available to legitimate users. In vehicular networks, this is a very serious situation on roads, where the channel becomes jammed and vehicles may not be able to communicate with each other. The system should be seamless so that life critical information reaches users on time.

3.6 Why classification is important in VANET packets

The classification of traffic is important in VANET in order to identify and differentiate between the intruder (malicious) and the victim (good). This can be done using multiple machine learning techniques. Classification is essential as it is a tool to single out and separate the intruders and stopping communication between the intruder and VANET. All data and information in the network would be secure as the intruders are unable to access the network and this prevents it from being hacked. This proactive measure should be carried out continuously to ensure security in all types of vehicle communications. Nodes can be

classified into passive and active nodes; the passive node does not communicate regularly and uses the network only for certain purposes and periods. Active nodes have good quality communication with VANET. These active nodes would then be classified into either malicious, or legitimate. Therefore classification of nodes is essential in VANET environments. One of the ways to classify nodes is by using an algorithm called Support Vector Machine, a learning algorithm that can predict the behaviour and conduct of nodes in VANET

The messages can be classified into categories such as type, importance, frequency, urgency, space and bandwidth required. Traffic messages can be categorized into accident messages, passerby messages, collision messages, emergency messages, traffic jam messages and road condition messages. Each message established should be given an ID to be identified with, along with the properties and tags for the nodes to make decisions about the transmission method, resources allocated, response time and responses such as authenticating, forwarding, discarding and operating. Classifying the messages optimizes the system's performance and provides stronger defense and security measures against potential threats and attacks.

Classifying nodes are also important in terms of enhancing the purpose of using VANET, which is to bring users more convenience and sense of security physically and digitally. Vehicles such as ambulances and fire trucks should be classified as vehicles that require higher priority; heavy vehicles such as buses and lorries which are able cause more hazards in the event of accidents should be classified with an ID so when they are near to other vehicles, the other vehicles can be more cautious The same situation applies to fast cars such as racing cars which in the event of collision could cause disaster. Combining with the software used inside cars, vehicles with notable features such as containing infants,

malfunctioning car parts and extra-long chassis can be recorded and classified and be utilized when sending safety messages to the drivers to enhance driver experience.

3.6.1 Impacts of Attack

VANET attacks can also be classified according to their impact. The primary impact is in the undetected attack, since communicating vehicles are inaccessible or there are a lot of malevolent vehicles nearby. The subsequent impact may able to detect the attack, nonetheless they are not fully altered since they lack information collected by vehicles. The third impact is on communication vehicles that received inaccurate information and might persist incorrectly for some time. Last but not least, the attacks can be noticed and modified by vehicles then they are associated with a huge number of truthful remote nodes. The remote nodes can check the received information and identify weather it is correct or not.

3.7 Why DoS and DDoS attackers attack safety applications

VANET used open wireless medium. Due to that there will be a number of attacks in the network. There is extremely high probability of attack. The main idea of the attacker is to create the trouble for the genuine node or user. Consequently, the services are not available which accomplishes the goals of the DoS and DDoS attack.

- **DDoS attack** the main purpose of the attacker is to bring down the network like with DOS attacks. Consequently, the attacker may attack both infrastructure and vehicular nodes. In the safety applications the time is very important because the user needs to get the accurate information on time without any delay. Time is very critical in any application. Safety application time critical application which require send to the user on time otherwise a major accident will occur. In this attack, attackers without manipulating the genuine content may

add some time slot to make a delay in the communication, and due to this the user will get the message after the required time. Normally, the safety application will send a life critical message and provide the warning message to another node. The attacker intended to modify the content of the genuine message and send the wrong message to other vehicle which causes accidents. Safety-application attacks may lead to vast numbers of deaths, while as this is not the case with non-safety application attacks. DDoS attacks achieved by internet botnets. On that time road sections are flooded with physical traffic. In the Internet the DDoS attack happen in the political incentives and economic purpose. For instance, it can be used in circumstances as thoughtful as deferring police arrival or reaching a robbery scene, hindering emergency vehicle entrance to a zone under a terrorist attack, or something as unassuming as collective overcrowding around a particular store to favour its competitor. Attacks can be classified as destructive/ malicious/ profit oriented or "just for fun". Malicious reasons would be intended to provoke accidents, to trouble other drivers or to cause traffic jams. Overall the amount of determination that an attacker is willing to devote to such attacks can be projected to be rather low. However, the level of determination will be higher if the attacker's aim is to become famous, to make a profit or to cause damage to vehicles. Visibly profit oriented motivations include freeing the road or a single lane along a particular route, redirecting the road traffic, or making drivers redirecting around designated locations such as a specific gas station.

The VANET is a new technology to implement and to improve road safety using ITS. There are many researchers working on security issues under VANET. The security issue on VANET was triggered at danger level in mid-2000 and openly bloomed in the year 2009. There is a large number of publications published since 2009 to 2019 related to VANET

security and attacks. That had made a substantial involvement to the enhancement of VANETs security and attacks.

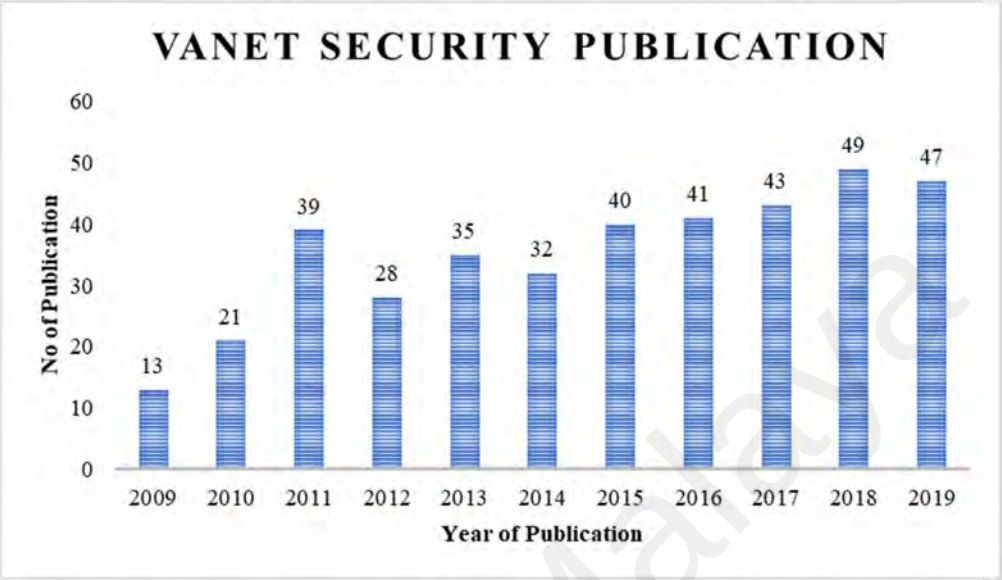

Figure 3.5: VANET Security Publication Statistics

In this part we have conducted the survey on security and attacks in VANET. Figure 3.5 indicates publications from 2009 to 2019. The author has searched in six main technical publishers/journals, including ACM Portal, IEEE Explore, Wiley Inter Science, ScienceDirect, Elsevier and Springer Online Library. The author used keywords to search abstracts and titles. Mainly, searches were carried out on VANET's vulnerabilities, VANET's security and VANET's attacks. The author does further search on the six databases for DoS and DDoS attack detection methods in VANET. Figure 3.6 shows the publication statistics on DoS and DDoS attacks in VANET. There is a limited number of articles on DDoS attack detection on VANET in the last five years. That has led the author to do research on DDoS attack detection methods on VANET.

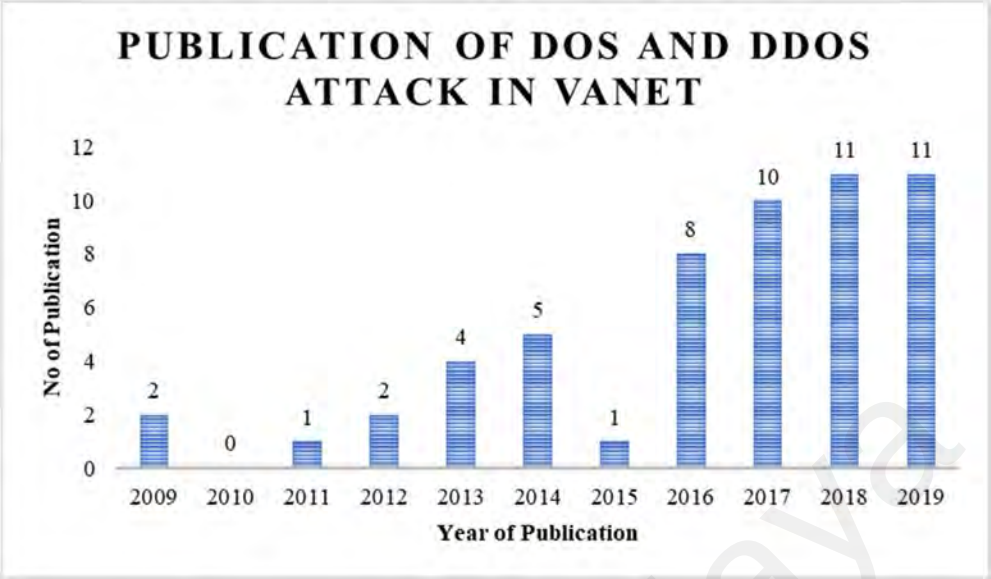

Figure 3.6: Publication Statistics of DoS and DDoS attacks in VANET

3.8 Conclusion

In this chapter, an in-depth analysis of all the problems encountered using DoS and DDoS attack was discussed. The taxonomy, tabulations, and statistics with regard to the relevant research efforts were also presented and discussed. The focus of this research was motivated by the quantitative and systematic review of existing techniques discussed in Chapter 2. Therefore, few of the issues that have been discussed in this chapter have been solved using proposed techniques and are further described in the following chapters.

CHAPTER 4: DDoS ATTACK DETECTION FRAMEWORK FOR VEHICULAR COMMUNICATIONS

4.1 Introduction

In this Chapter, the methodology for a DDoS attack detection framework for vehicular communication is disscussed and the algorithms will be explored. In addition, the requirements for the framework and the model's method will be elaborated. In a later section, the discussion will focus on the design and implementation of the model. Finally, the architecture and components of classsification will be explained in detail.

4.2 VANET Scenario

The VANET scenario is illustrated in Figure 4.1

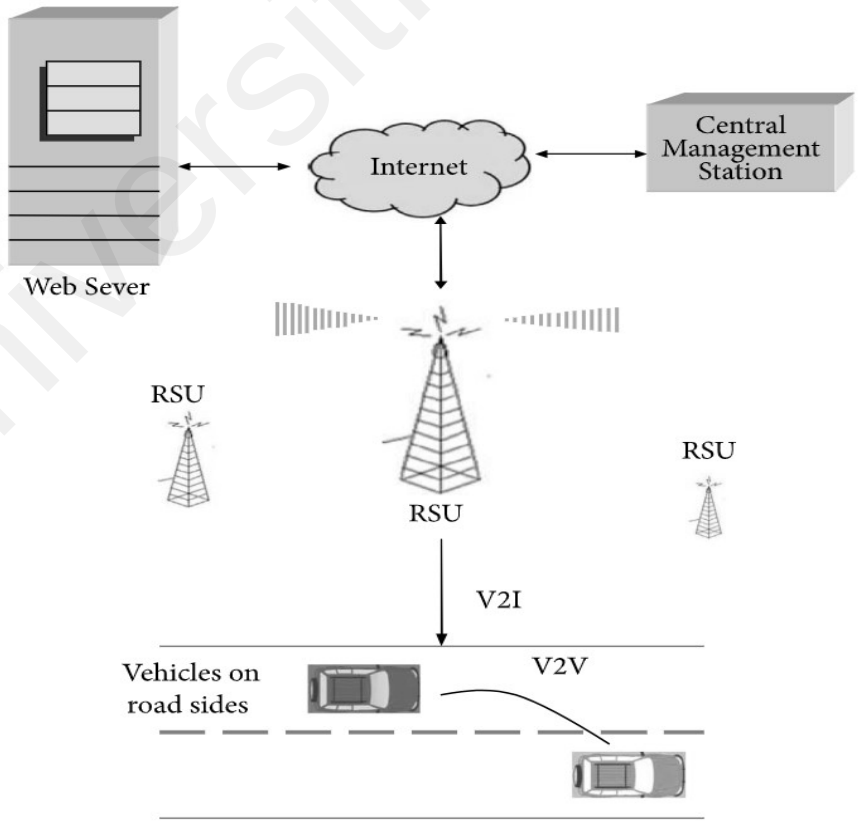

Figure 4.1: VANET Scenario

The web server handles the instruction nodes in the RSU through the Internet. A main central management station maintains all the overall RSUs. The RSU notices accidents occurring and messages are passed through vehicles in V2I communication. The V2V denotes the Vehicle-to-Vehicle communication taking place between the vehicles. Applications of VANET vary in their requirements according to the timeliness of data delivery. The reply time is for the follow-up of accident avoidance in the neighborhood or barriers on the road. Reply time tolerates minimum delays for the route optimization models. A minimum delay is acceptable in noncritical delay-tolerant activity mechanisms.

4.3 Research Methodology

The methodology of this proposition includes three main phases, namely:

(i) Literature review and problem analysis.

(ii) Design and development of DDoS attack detection framework for vehicular communications in VANET

(iii) Validation and statistical analysis of the projected model

The *literature review and problem analysis* – the literature review discussed our understanding of the rudimentary knowledge of VANET and its architecture. Also, the state-of-the-art of DDoS attacks was also discussed along with existing DDoS attack detection methods as well as other methods. The problem analysis covers a deep understanding of the actual problems of the DDoS attack in the vehicular communications in VANET. Chapters 2 and 3 covered the literature review and problem analysis.

The second phase is *design and development of the DDoS attack detection framework* – this phase focuses on detection methods for DDoS attacks in VANET vehicular communication.

However, the implementation and problem formulation use a network simulator. There are two models being proposed under one framework. The first model is Multi Variant Stream Analysis , where the method will identify and classify the packet according to the importance of the packet before it is blocked/dropped. By using the computed stream weight, the method will classify the packet as malicious or genuine. The attacker's behaviour will be reduced by the proposed technique. Malicious vehicle node formation is minimized. The first model is used on a small scale such as less number of vehicles on the road, i.e. < 50 vehicles. The second model is a Stream Position Performance Analysis. This is a cluster-based environment suitable for larger scale V2V communications. In this model, the attack severity level will identify whether the attacks are high impact or low impact. The SPPA model is considered as cluster-based attack detection, in data collection where the leaf nodes pass the sensitive information to the cluster head. In conclusion, the outcome of the proposed model evaluation results increases the packet delivery ratio and improves the detection time and overall throughput. This phase resembles the second objective of this research. The output of both models has been published by the author and is included in the literature review.

Finally, *Verification and validation* – in this stage the author primarily focused on assessing the proposed models using 7 performance metrics such as Attack Detection Time, Attack Detection Rate and False Classification Ratio, Throughput, End to End Delay, Packet Delivery Ratio and Routing Overhead. All the 7-performance metrics will be evaluated with existing DDoS attack detection performance metrics. The results from the Ns2 simulation will be validated by using statistical tools. The statistical package used for the analysis is Mini Tab Version 18. Analysis includes descriptive statistics and an Anova test supported by the Tukey comparison test to detect significant differences among 5 models. Moreover, to apply and evaluate the proposed techniques is the result of the earlier stage – (research

objective 2) in the detection of DDoS attacks on VANET vehicular communications. The research methodology has been summarized in Figure 4.2.

Furthermore, the following sections discuss the proposed DDoS attack detection model for vehicular communications, to address some of the problems specified in the earlier chapter. The results and graphs from the all the two models have been discussed in the Chapter 5. The proposed model by the author shows good results from the Ns2 simulation results from the validation and signification. The limitation of this work is that it may not able to detect other attacks in the VANET environment. This will be addressed in the future direction part of Chapter 6 and the author will use ant colony optimization and the framework will become a hybrid or enhanced model.

Phase 1: Literature Review & Problem Analysis

Principles/Overview Of VANET	VANET DDoS Detection Method
VANET Components	Novel Security Approach for Data Flow and Data Pattern
VANET Technology	Novel Traffic Congestion Detection and Removal Scheme Against DDoS Attack
VANET Characteristic	Sentinel: Defense Mechanism
VANET Limitation	A Group Adaptive Controller-Based Method
VANET Challenge	Attacked Packet Detection Algorithm (APDA)

Phase 2: Design and Development of DDoS Attack Detection Framework for Vehicular Communications in VANET

Multi Variant Stream Analysis Model	Stream Position Performance Analysis Model
Incoming packet	Incoming Packet
Classification	Cluster Head Selection
Pre-Processing	Stream Position
Multi Attribute Stream Weight (MASW)	Conflict Field, Conflict Data, Attack Signature Sample (CCA)
Packet Marking	DDoS Attack Detection
DDoS Attack Detection	Attack Severity Level

Phase 3: Verification and Validation

Evaluation Metrics	Simulation Setup	Statistical Analysis & Performance Evaluation
Detection Time	PARAMETER / VALUE	Mini Tab (Ver 18) Statistical tools
False Classification Ratio		
Attack Detection Rate		
Packet Delivery Ratio		
Routing Overhead		
End to End Delay		
Throughput		

PARAMETER	VALUE
Platform	Ns2.34
Topology Size	1000m * 1000m
Packet Size	512 Bytes
Simulation Time	200 Sec
Node Speed	30 m/s
Number of Nodes	15, 30, 45, 60, 75, 90, 105, 120, 135, 150
RSU	3
MAC Layer	IEEE 802.11p
Antenna Model	Omni-directional Antenna
Data Transmission Range	20 Mbps
Bandwidth	2 Mbps
Mobility Model	Random Way-Point

Figure 4.2: Overall Framework of the Research Methodology Process

4.4 DDoS Attack Detection Framework

The proposed DDoS attack detection framework consists of 2 models. The first model is Multi Variant Stream Analysis and the second is Stream Position Performance Analysis. The MVSA model deals with small scale environments. However, the second model deals with large scale environments. The MVSA model consists of several stages, namely classification, Pre-Processing, Multi Attribute Stream Weight (MASW), Packet Marking and DDoS Attack Detection. All the MVSA stages are well explained in section 4.4.1. The SPPA model consists of Cluster Head Selection, Stream Position, Conflict Field, Conflict Data, Attack Signature Sample (CCA), DDoS Attack Detection and Attack Severity Level. All the SPPA stages are well explained in section 4.4.2.

4.4.1 Multi Variant Stream Analysis (MVSA) Model

VANETs are considered as one of the most prominent technologies for improving the efficiency and safety of modern transportation systems. However, the VANET is also subjected to attacks that will weaken the performance of vehicular communications. To enable communication inside the VANET system, a routing protocol helps to determine directions among nodes. In VANET networks, nodes move very quickly from one place to another, and in that time, DDoS attacks will occur in the VANET network. Therefore, it is important that we implement the DDoS attack detection-based communication level on the entire system. The source node will send data to the destination using intermediate nodes, at that time any DDoS attack will happen in the node. Dealing with these attacks in VANET is a challenging problem. Most of the existing DDoS detection techniques suffer from attack detection time, packet loss and incur high computational overheads. To cope with this problem, we present a novel MVSA method. In this approach the incoming packet from V2V and V2I will capture the packet log and send it to the classification stage. In the

classification stage, the traffic will identify whether it is safety application traffic or non-safety application traffic. Once the traffic is identified, it will go through the preprocessing stage.

Once done with the classification process, the preprocessing will generate rules at the boot time using the network trace. However, the method will read the incoming packet from the classification and split the trace into classes. One frame is identified for each class, and the method will split the records using traces. The preprocessing will compute the payload, Hop Count, Compute Time to Live and Packet Frequency. All the four features will compute to generate the rules. The generated rules will be used to perform a DDoS attack detection in the DDoS attack detection stage. The multivariant stream factor will help to compute each time window. By using computed multivariant stream factors, the method will compute the MASW. Computed stream weight will be used to perform DDoS attack detection. Followed by packet marking, which is used to trace back to the source node, then the node of origin used in RSU for data request and data will get a response in the network This method shows that there is no modification in current routing methods during the data transfer. Finally, in the DDoS detection stage, the rules from preprocessing, packet marking and MASW will be used to classify the affected packet from the VANET environment.

The Multi Variant Stream Analysis Model and its functional components are shown in Figure 4.3. Due to the rapidly changing network topology, frequent exchange of information and high mobility, the detection of DDoS attacks is more challenging (Sharma & Sharma, 2017). The MVSA method classifies the traffic into classes based on the type of application. The traffic class classifies them into two classes: first, safety application traffic and second, non-safety application traffic. Conversely, for each class there is a different rule.

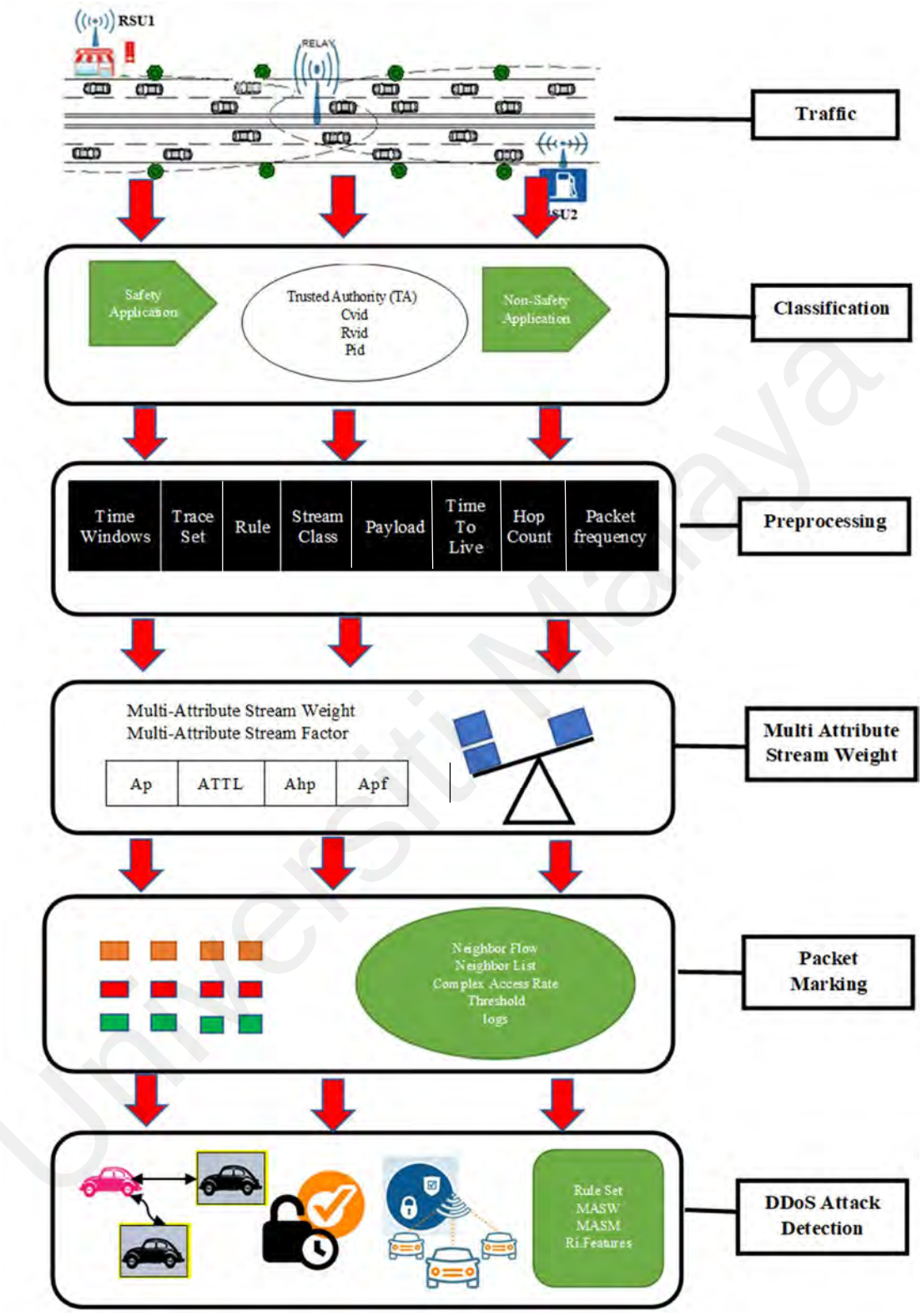

Figure 4.3: Proposed Multi Variant Stream Analysis (MVSA) in Vehicular Communications

The rules will be generated according to the number of time windows used, ranging from 1 to 24 it shows in the section 4.4.1.2. The rule will verify the incoming traffic and computes the Multi-Attribute Stream Weight for the incoming packets. The computed Multi-Attribute Stream Weight outcome will use in the detection stage (it is clearly explained in section 4.4.1.3). Then the process will continue with packet marking stage (it is clearly explained in section 4.4.1.4). Finally, the DDoS attack detection stage is clearly explained in section 4.4.1.5.

In the MVSA model, four parameters are used. The first is "Payload" which refers to the amount of data present in the packet. The second is "Hop Count," which refers to the number of intermediate nodes a message must have to pass through to reach the destination. The third is "Time To Live (TTL)," which refers to the lifespan of data in the transmission route or network. However, each data packet has some fixed TTL which is fixed by the MAC layer and the protocol being used. It is also fixed according to the number of hops it has to travel according to the Hop Count. If the packet reaches the destination after the mentioned TTL, then the value is considered as modified or spoofed. So, by counting the TTL value, the chance of being modified can be identified. Nevertheless, if any intermediate node tries to modify or learn the packet features then it will take some time, and it would cross the specified TTL value. Finally, is the "packet frequency," which is about sending several packets at a particular time. For example, "in one minute how many safety application traffic packets have been received and calculate the total number of packets received for safety applications" Table 4.2 shows the abbreviation of the algorithm.

4.4.1.1 Classification stage

In the classification stage, the process will identify the safety application traffic packet and non-safety application traffic packet. In VANETs' safety applications, vehicles broadcast two types of messages: warning (event driven) and status messages. Warning messages usually contain safety critical information and have to be propagated from one hop to the next until they reach a certain distance in a very short time to avoid chain collisions. Status messages are sent periodically to all vehicles within their range only and contain a vehicle's status information such as speed, acceleration, direction and position (Hafeez et al., 2010). The classification will check the vehicle ID whether it is registered with a trusted authority or not. If it is registered then the classification will continue to check the packet size; if the packet size is less than 2000 bytes then it is considered a safety application (Hafeez et al., 2010) and if the packet size greater than 2000 bytes it is considered a non-safety application. The algorithm is as follows:

```
If (RVid=CVid)
 {
  Alert message ("yes");
  //Continue to classify the packet
   For (j=0; j<Pid;j++)
  {
        Int d= Size of (Pid);
        If (d<=2000)
                {
  Alert message ("Classify as safety application packet");
}
    Else
{
    Alert message ("Classify as non-safety application packet");
```

Where *RVid* is Registered Vehicle id and *CVid* is Current Participating Vehicle id. Moreover, *Pid* is Packet ID and *d* is data. Nevertheless, in some situations where the vehicle ID did not register with the trusted authority, then the vehicle packet will be dropped. The process will identify the importance of the packet and it will be sent to the pre-processing stages. Refer to the flow chart of the classification stage shown in Figure 4.4.

4.4.1.2 Preprocessing Stage

In the preprocessing stage, the network trace is maintained by the node which performs DDoS detection. It is just a log of packets received from different source nodes which contain all the information on the features considered in this model. Each packet received will be processed for classification, because the rule is generated at the boot time using the network trace. At the next boot, the detection node will generate the rule. The equation for rule is shown below:

$$\textit{Generate Rule (Gr)} = \{Ti, Si, Ap, Ahc, Attl, Apf\}$$

$$\textit{Add to Rule Set (Rs)} = \sum(Si \in Rs) \cup Gr \quad \text{Eq. (1)}$$

Where *Ti* is time window, *Si* means stream class, *Ap* means average payload, *Ahc* is average hop-count, meanwhile *Attl* means average time to live and *Apf* means average packet frequency. The generated rule will be stored in the set. Conversely, the algorithm will compute the rules to perform DDoS attack detection in the DDoS attack detection stage. The flow chart for the preprocessing stage is shown in Figure 4.5. The explanation of flow chart, the process is continuing from classification and followed by preprocessing. In the preprocessing stage the first step will read the network trace (NT) and split the trace into different time windows. The equation for trace set is shown below:

$$Ts = \int_{Ti=1}^{24} Split(Nt, Ti) \quad \text{Eq. (2)}$$

Where Ts means Trace Set. It will split the network trace into different Time Windows (Ti). Moreover, for each Time Window (Ti) from Trace Set (Ts) Compute payload, Compute Hop Count, Compute Time to Live and Compute Packet Frequency. The equation for Payload, Hop Count, Time to Live and Compute Packet Frequency is shown below:

$$\frac{\sum Ts(Ti,Si).payload}{size(\sum Ts(Ti,Si))} \quad \text{Eq. (3)}$$

$$\frac{\sum Ts(Ti,Si).hop\ count}{size(\sum Ts(Ti,Si))} \quad \text{Eq. (4)}$$

$$\frac{\sum Ts(Ti,Si).TTL}{size(\sum Ts(Ti,Si))} \quad \text{Eq. (5)}$$

$$\frac{\sum Ts(Ti,Si).Packet\ frequenc}{size(\sum Ts(Ti))} \quad \text{Eq. (6)}$$

Once computed, then the process will generate the rules and add the Rule Set (RS) in the DDoS detection stage. The parameters and its functions are shown in Table 4.1.

Table 4.1 Parameters and Its Functions

Parameter	Function
Payload	The Payload, which refers to the amount of data present in the packet. On the other hand, the service providing node can accept only a limited amount of data at any point in time, and when it receives a higher payload data packet, it suffers from overload. This high payload data also affects the performance of the V2V communication.
Hop Count	The Hop Count, which refers to the number of intermediate nodes a message must has to pass through to reach the destination. Moreover, the number of hops affects quality of the route. To save bandwidth, which is precious in VANETs, it is important to select a route with a minimum number of nodes.
Time to Live	The Time-To-Live (TTL), which refers to the lifespan of data in the transmission route or network. However, each data packet has some fixed TTL which is fixed by the MAC layer and the protocol being used. It is also fixed according to the number of hops it has to travel according to the Hop Count. If the packet reaches the destination after the mentioned TTL, then the value is considered as modified or spoofed. So, by counting the TTL value, the chance of being modified can be identified. Nevertheless, if any intermediate node tries

	to modify or learn the packet features then it will take some time, and it would cross the specified TTL value.
Packet Frequency	Packet frequency is about sending several packets at a particular time. For example, in one minute how many safety application traffic packets have been received and calculate the total number of packets received for safety applications.

4.4.1.3 Multi Attribute Stream Weight (MASW) Stage

The MASW is the third step after the preprocessing step. It is not necessary for the vehicle to read the trace; a single node may be a vehicle which reads the trace and computes the value. The network trace will specify the traffic type and compute the MASF. The MASF is computed for each time window. By using the computed MASF, the method computes the MASW. The computed MASW will be used to perform DDoS attack detection in the DDoS attack detection stage. The flow chart for the Multivariant Stream Weight Stage is shown in Figure 4.6. In the flow chart, the process is continuing from preprocessing and is followed by the MASW stage. In the MASW stage, the first step will read the network trace (NT) and for each time window (Ti) it will compute the payload, compute the Hop Count, compute the Time to Live and the Average Packet Frequency. The equation is shown below:

$$\bar{x} = \frac{\sum Ts(Ti)x}{size(\sum Ts(Ti))} \ , x = Ap \mid Ahc \mid Attl \mid Apf \qquad \text{Eq. (7)}$$

For each Time Window, this algorithm will compute the payload, hop count, TTL value and packet frequency. Once computed, all four parameters then continue to compute the MASF. The equation is shown below: -

$$MASF = (Payload / Packet\ frequency) * (Hop\ count / TTL) \qquad \text{Eq. (8)}$$

Finally, the MASF is divided by (T) into hours, meaning the denominator (24) is the entire time value, which is split into the number of the time window. For example, if the class splits time (24) into 1 hour then we will get a 24-time window. This computed weight will be used in the DDoS detection stage. The equation for MASW is as below: -

$$MASW = (MASF) /T \quad \text{Eq. (9)}$$

4.4.1.4 Packet Marking Stage

The packet marking stage uses space limitation to determine packet marking by demanding that a container is labelled with only a part rather than the whole of the path it traverses. Packet marking incurs little overhead when routers mark packets at a low marking rate, but the victim vehicle needs a large number of packets to reconstruct the path to the source vehicle. It is more suitable for flooding attack trace back and cannot locate a single packet. The object matches packet marking with the routers on the region and it is easy to recreate the attack track.

A single node fault in systems is typically insignificant if it does not lead to a loss of sense and message coverage. The VANETs are leaning towards personal communication and damage the connectivity to important nodes. There are some issues in the design of nodes in the routing protocol. At first, the node implants its trust value on the session request and sends it to the server. If valid, it forwards the request. Otherwise, the node is considered as suspicious and dropped. The flow chart for the Packet Marking Stage is shown in Figure 4.7. To explain the flow chart, the process continues from the MVSW stage and is followed by the packet marking stage. In the packet marking stage, the first step will check the initial flow and the neighbours, then for each neighbour flow (Ni), first it extracts the neighbour

log file then extracts the Collective Flow which is then present in the Neighbour List (NL). The equation is shown below:

$$For\ each\ Ni \mid Extract\ logs\ Nl = \int \times flow\ ()1 \mid Extract\ collective\ Flow\ present\ in\ Nl \quad \text{Eq. (10)}$$

Where Ni is Neighbour Flow and Nl means Neighbour List. First, the neighbour log file should be extracted, and the equivalent to the flow of the initial node should be integrated. Moreover, the collective Flow collects the number of neighbour nodes called 'flow'. Once extracted, for each path (p) from Neighbour (Nr), calculate the Complex Access Rate (CAR), which fully depends on the Access Data. The equation for the CAR is shown below:

$$CAR = \int (*target\ flow)/NR \mid CAR\ (i) = AD(i) + TR. \quad \text{Eq. (11)}$$

CAR means Complex Access Rate and NR means Neighbour Vehicle. If there is any return NR value that should be considered for the Neighbour List (Nl), the CAR value is calculated, which fully depends on the Access Data, AD. The process will continue to check if CAR (Ti) > threshold, then it will Mark the source address of the region as a malicious node region. The equation is shown below:

$$\begin{aligned} &For\ respectively\ Time\ window\ (Ti) \\ &If\ CAR\ (Ti) > Threshold \\ &Suggestion = false \end{aligned} \quad \text{Eq. (12)}$$

After that, to calculate the CAR value based on the network density, if the value is less than the threshold, this means select the source address of the particular region in the network. Continue to add the vehicle node address to the malicious list. The equation is shown below:

$$Ml = \Sigma\, flow\ (Ml) + TR. \quad \text{Eq. (13)}$$

Ml means Malicious List and TR means Trace. It will mark the source address of the region as a malicious node region and adds the node address to the malicious list. Finally, if the CAR (Ti) Value is Less Than Threshold, Select the source address of the particular region in the vehicular network and continue with the DDoS attack detection stage.

4.4.1.5 DDoS Detection Stage

The DDoS detection stage is the final step in the MVSA approach. In this stage, the node first reads the network trace from the neighbour location and preprocesses the logs. The preprocessing algorithm returns the set of rules. As for the received packet stream, the method will compute the multivariant stream weight, by using the rule set generated and stream weight computed, and the method will classify the affected packet. The flow chart for the DDoS attack Detection Stage is shown in Figure 4.8. The flow chart shows that the process is continuing from the packet marking stage, followed by the DDoS attack detection stage. In the DDoS attack detection stage, the first step will read the NT and add the rule set from the preprocessing stages. Then it will continue to compute the MASW, from MASW stage and add the outcomes from the packet marking stage. Once computed then it will check the Multi-Attribute Similarity Measure (MASM). The equations for MASM are as follows:

$$MASM = \frac{Dist(Ri.Pl,P.Pl)}{\sum Packets\ receievd\ in\ Ti} \times \frac{Dist(Ri.hc,P.hc)}{P.ttl} \quad \text{Eq. (14)}$$

To compute the similarity, the computed value will be considered. However, the computed value for the received packet should fall within the measure of rules that are available for the specific time window. The algorithm must compute the distance between the rules and the features extracted for received packets. Finally, the process will classify as true, otherwise it will be classified as malicious and the packet will be dropped. The equation is shown below:

$$MASM < MASW \;\&\&\; MASW < > Ri.Features \qquad \text{Eq. (15)}$$

The “Ri.Feature” means the feature that is used to detect DDoS attacks. The algorithm has many features in the rule such as average packet frequency, average payload, average TTL and average hop count. The MASM and MASW are computed according to the mentioned features only. Based on that the decision will be taken.

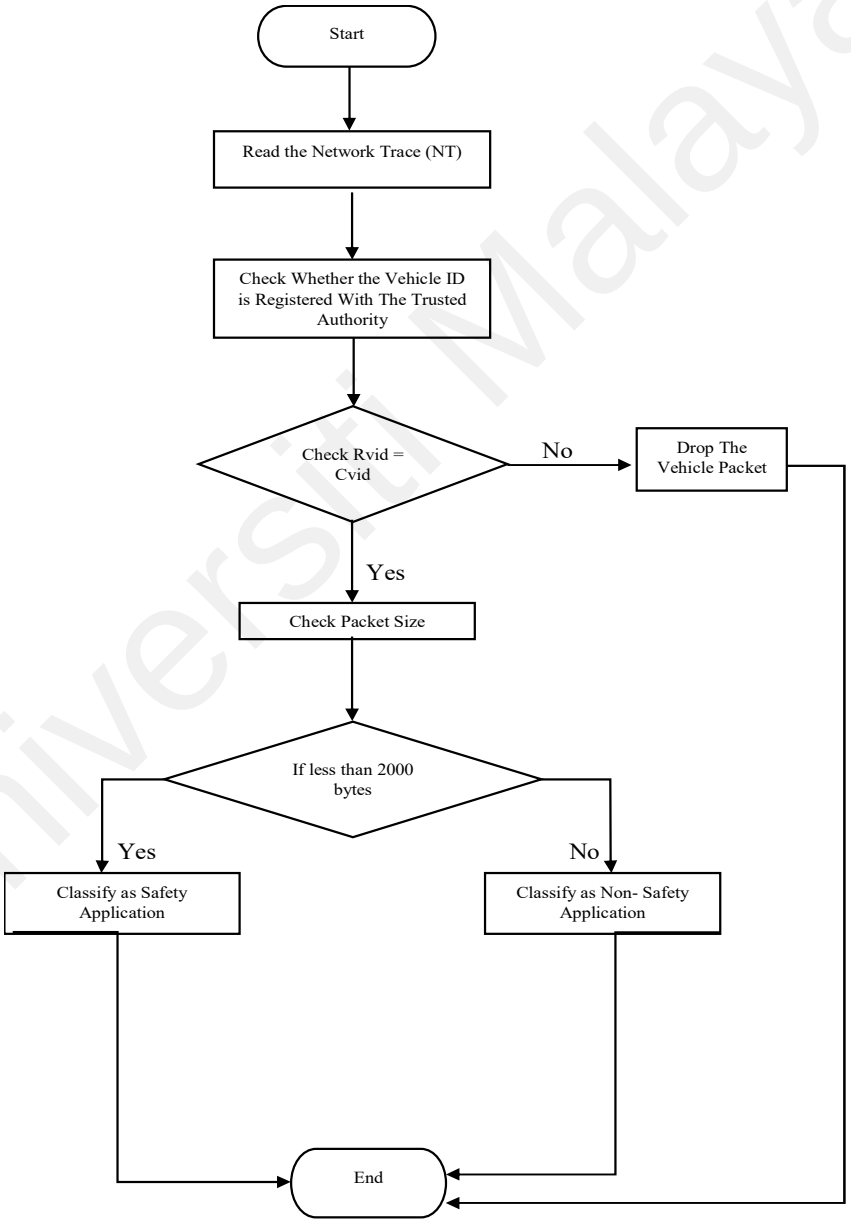

Figure 4.4: Flow Chart for Classification Stage (MVSA)

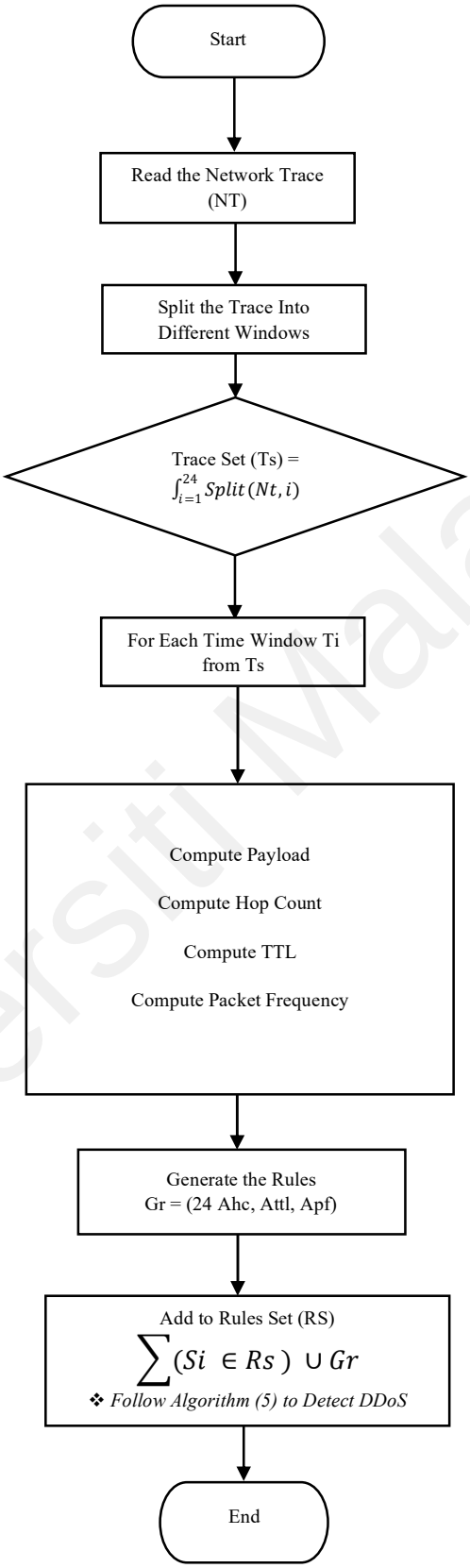

Figure 4.5: Flow Chart for Preprocessing Stage (MVSA)

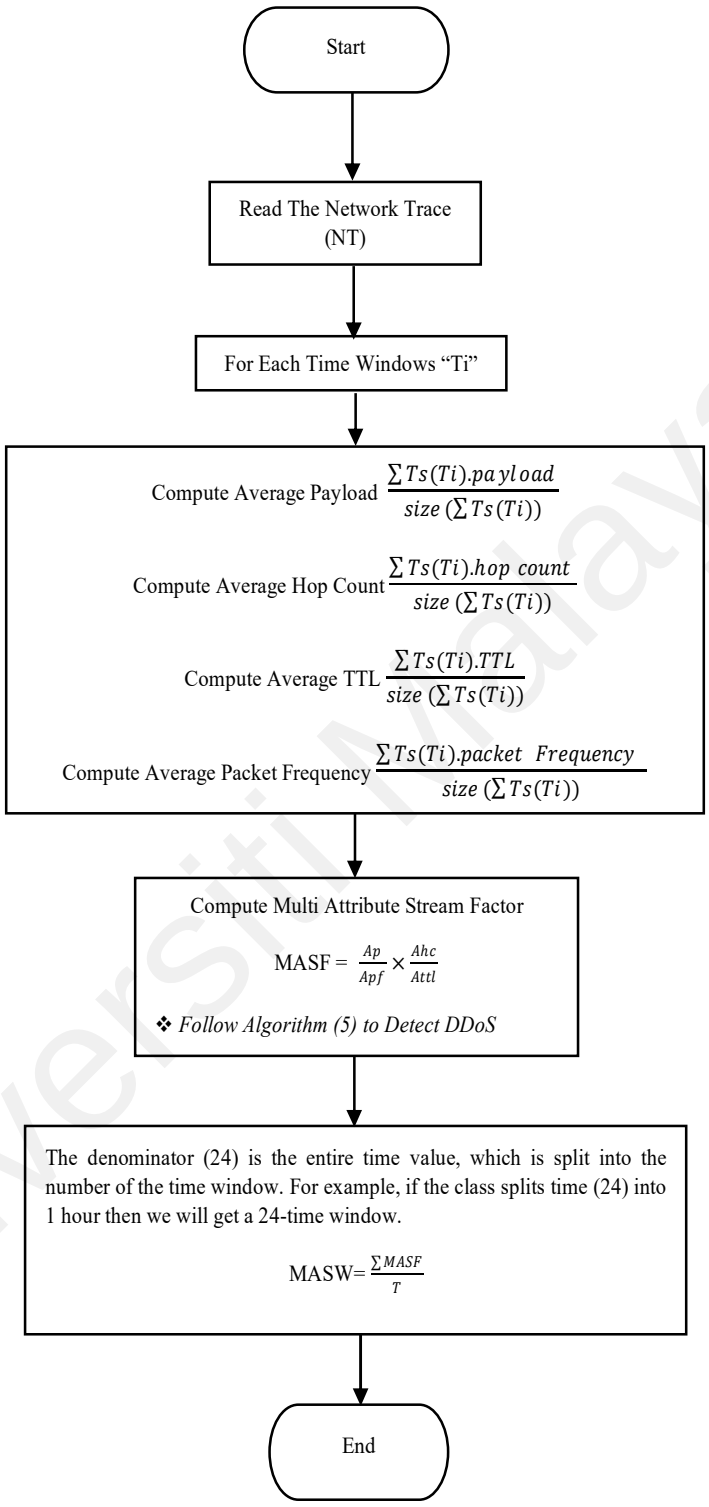

Figure 4.6: Flow Chart for Multi Attribute Stream Weight Stage (MVSA)

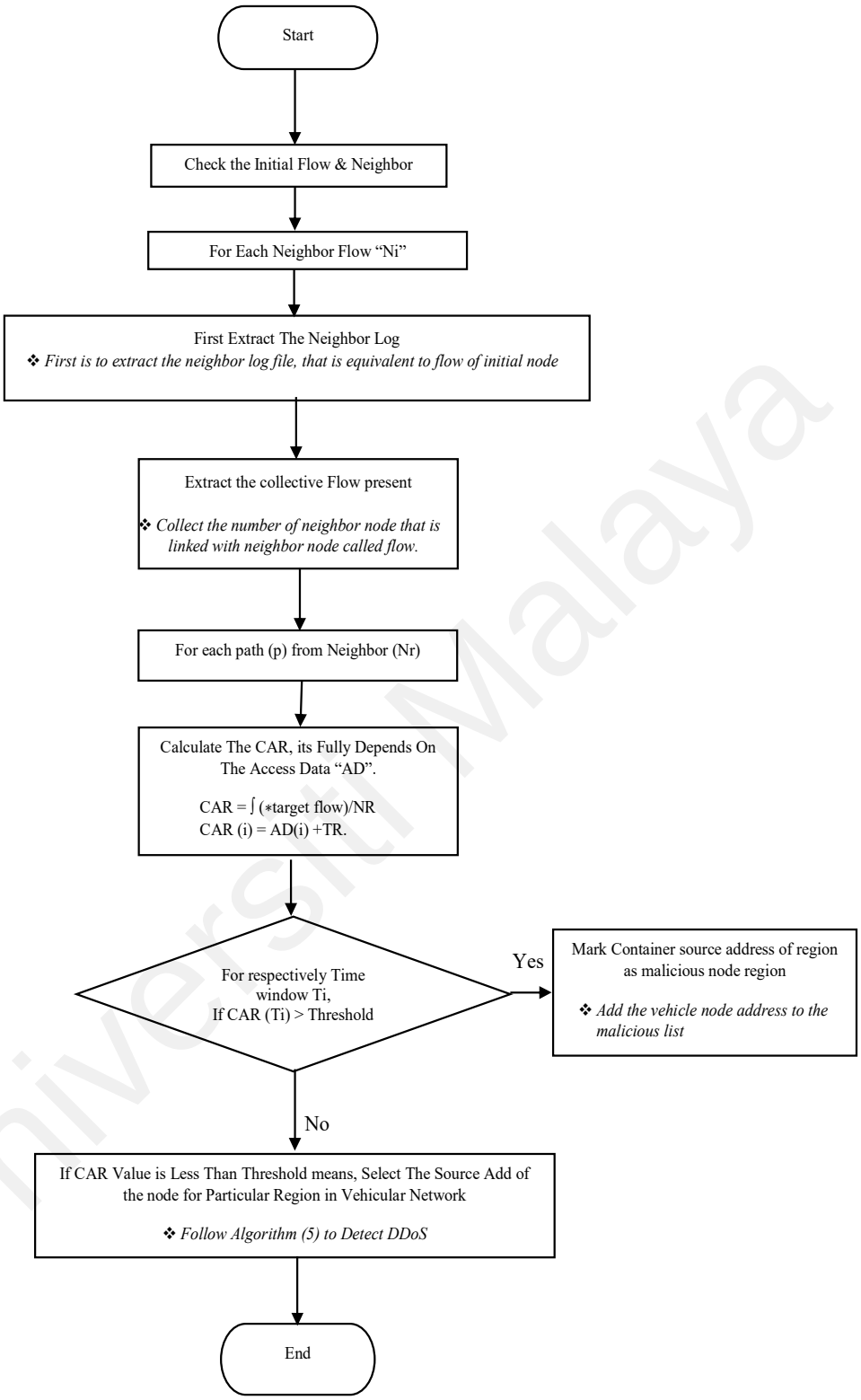

Figure 4.7: Flow Chart for Packet Marking Stage (MVSA)

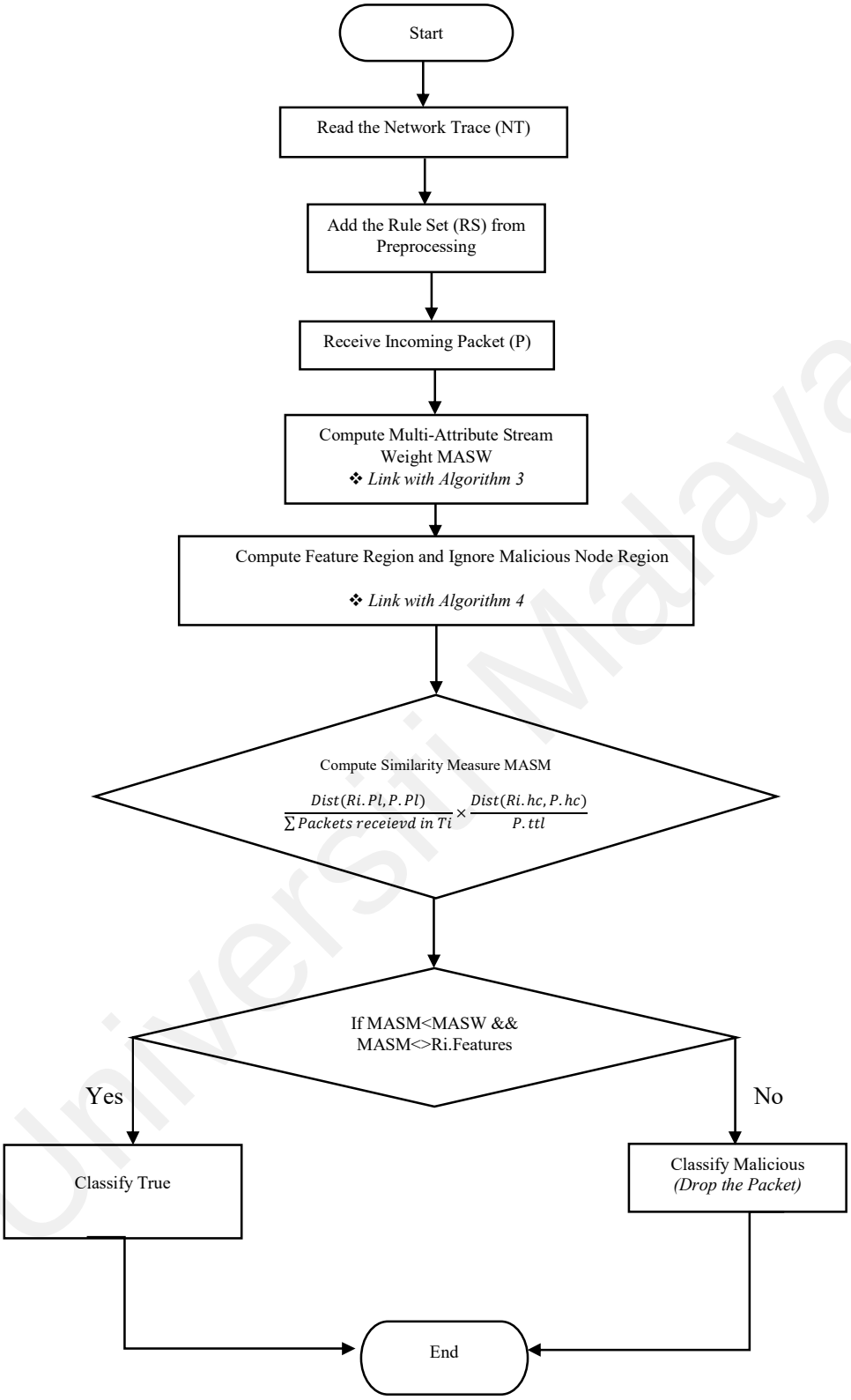

Figure 4.8: Flow Chart for DDoS Attack Detection Stage (MVSA)

Table 4.2: MVSA Abbreviations

Abbreviation	Meaning
CVid	Current Participate Vehicle id
RVid	Register Vehicle id
Pid	Packet ID
Nt	Network Trace
Gr	Generate Rule
P	Packet
Rs	Rule Set
Ri	Each Rule
Ts	Trace Set
Ap	Average Payload
Ahc	Average Hop Count
Apf	Average Packet Frequency
TTL	Time to Live
Attl	Average Time to Live
Ti	Time Window
Si	Stream Class
OD	Occurrence Detection
Ni	Neighbor Flow
Nl	Neighbor list
NR	Neighbor
CAR	Complex Access Rate
Ti	Time Window
M1	Malicious list
TR	Trace
AD	Access data
T	Time
MVSA	Multi-Variant Stream Analysis
MASW	Multi-Attribute Stream Weight
MASF	Multi-Attribute Stream Factor
MASM	Multi-Attribute Similarity Measure

4.4.2 Stream Position Performance Analysis (SPPA)

This section describes the second proposed method called the SPPA model to detect DDoS attacks in a large scale VANET environment. This model may help the large scale VANET environment in detecting DDoS attacks, regardless of the geographical location. In this model, the approach that was considered is a cluster-based DDoS attack detection by adopting one vehicle to be elected as a Cluster Head (CH) to control the communication in large scale VANET environments. The leaf node (vehicle) periodically updates the information of the critical zone (such as incidents that happened in the cluster zone) to its

CH. Hence, communication between the leaf node and the CH are performed through cluster-based routing, where the leaf node sends any sensitive information about its situation or its necessity to the CH. However, intruders might try to hack the information and send false information to the CH and from the CH to the centric controller. The centric controller takes responsibility for the entire node and performs decisions based on the necessity of the time of the attack detection.

A vehicular network is formed between clusters of vehicles. As vehicles move at high speed on the roads, the communication between them will break down frequently and the topology or interconnection between the vehicles will frequently change (Hasrouny et al., 2017). The network could be dense depending on the number of vehicles on the road and the comparative speeds at which they travel. Routing of messages between vehicles would need to overcome these topological issues and take into consideration the mobility and communication conditions (Panjeta et al., 2017). The dynamic nature of the topology would require frequent exchange of neighbour information to form the message routes leading to high communication overhead. Since the vehicles have high mobility, maintaining end-to-end connection between them would not always be possible.

Due to malicious activities, or the controller neglecting to take proper decisions, critical situations can happen in the VANET environment (Theresa & Sakthivel, 2017). To overcome this issue and to detect such malicious performance, a Stream Position Performance Analysis based attack Detection model has been designed. Figure 4.9 shows the architecture of the proposed SPPA model which highlights its workflow and its components. Each component has a unique work determination and has five primary stages, i.e. cluster head selection, stream position, CCA, attack detection and attack severity level.

The cluster head selection stage involves choosing the cluster nodes as well as cluster heads for data transmission.

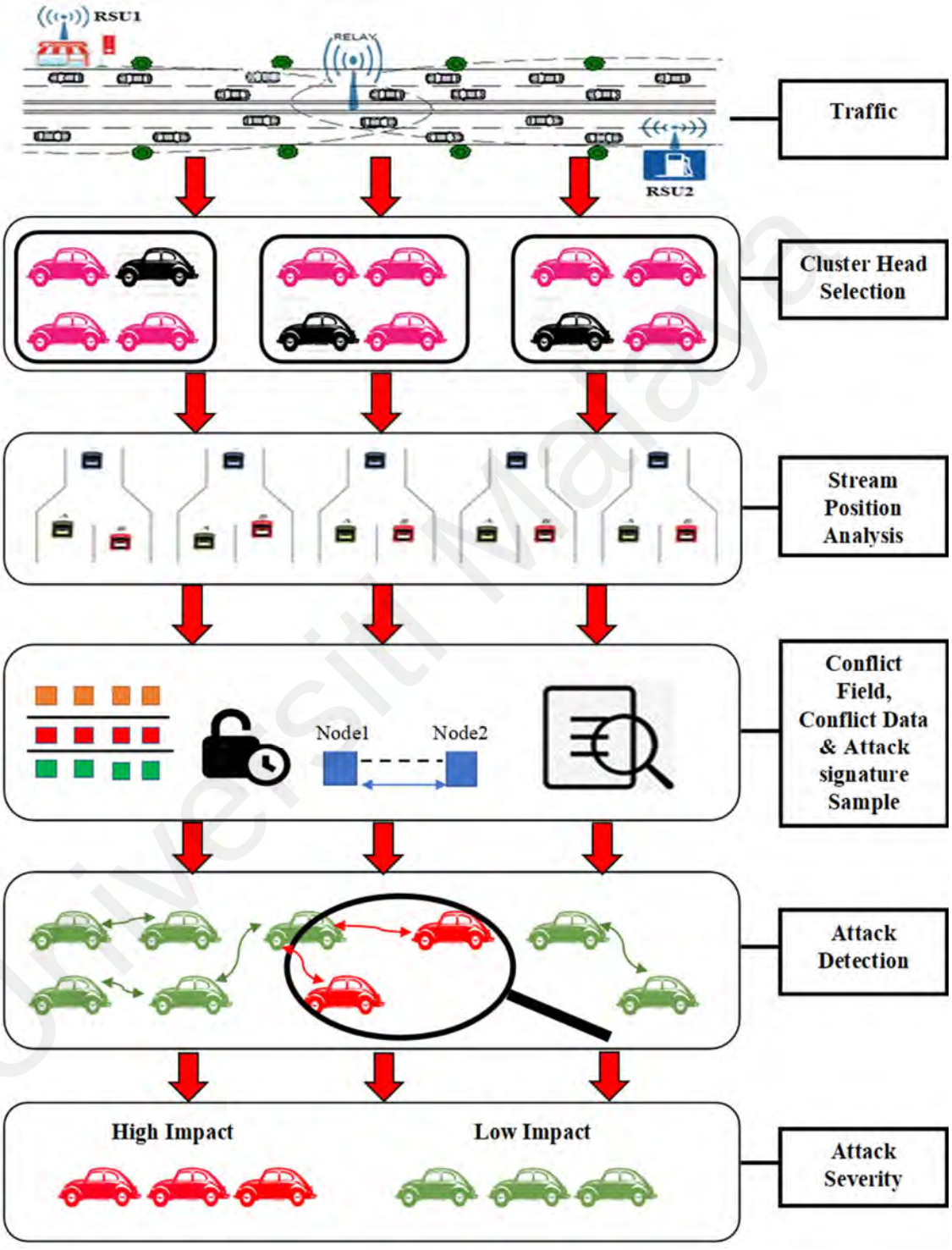

Figure 4.9: Proposed Stream Position Performance Analysis (SPPA) in Vehicular Communication

The stream position stage analyses the neighbour nodes for better service and data transmission in the network. The CCA is the third stage, where the node history is computed based on the calculation for detecting the attacker node in the network. Based on information from CCA, the attack can be detected in the fourth stage. Finally, stage five is where attack severity level is identified whether it's a high impact or low impact attack. Figure 4.9 shows the Stream Position Performance Analysis model. Table 4.3 shows an abbreviation of the algorithm.

4.4.2.1 Selection of the Cluster Head Stage

The CH is the most predominant node, with more energy and the most powerful among the nodes in the cluster. Each CH knows all information about its clusters and its leaf nodes. Initially, 1-hop clusters are formed by an assumption. Secure cluster heads are formed based on the clustering score. The node list is formed with neighbouring nodes. The v_i is focused on how many neighbours are available among the source nodes at that particular point of time and the chosen distance between the nodes. Clustering score v_i is found for individual nodes in the neighbouring list. Then, nodes are classified into suspect, attacker or normal based on the routing scheme. Suspect nodes are motivated by a reputation mechanism, and attacker nodes are not allowed to participate in the selection process. The process will check the weightage each time, as shown in Figure 4.10.

Furthermore, the neighbour node with the maximum v_i is selected as the cluster head. The data transmission is quickly done if there are high numbers of neighbour nodes available. If any error occurs in the process, then it is easy to choose another neighbour node as CH. It ensures that a node is not allowed a faulty claim in the clustering process. The flow chart for the Selection of Cluster Head Stage is shown in Figure 4.10. The flow chart shows the

process starting from the Cluster Head Stage. The importance of this process is to identify the packet with the maximum Variable Score (Vi) as a cluster head. The equation as shown below:

$$V_i = \{v_1, v_2, v_3 \ldots\ldots v_n\} \text{ Clustering variable Score} \quad \text{Eq. (16)}$$

$$N_L = \{n_1, n_2, n_3, n_n\} \text{ // node's Neighbour Lists} \quad \text{Eq. (17)}$$

At first the process will check the cluster size; if it is less than the neighbour list size, it will extract all the Neighbour List (NL). The equation is shown below:

$$\begin{aligned} &\text{If (Neighbour Lists size} > \text{Maximum Cluster Size) formerly} \\ &\text{Abbreviate } N_L \text{ in the direction of Maximum Cluster Size} \\ &\text{Category } N_L \text{ based scheduled Vi} \end{aligned} \quad \text{Eq. (18)}$$

Based on the neighbour list, choose the correct node to reach to the destination through the cluster size or list. If (Ni=3) neighbour is a suspicious node, compute the Vi. The equation is shown below:

$$\text{For all nodes i in } N_L \text{ if } (N_l = 3) \text{ Than the Neighbour is Suspicious Node "Compute } V_i\text{"} \quad \text{Eq. (19)}$$

The Vi is Variable Score (it is a boundary of 4 sides like north, east, west and south). Moreover, if (Ni=4), the neighbour node is a normal node, if cluster size is equal to the neighbour node size, the node is a normal node otherwise the node is a congestion node. The equation is shown below:

$$\text{if } (N_i = 4) \text{ Than the Node is Normal Node "Calculate } V_i\text{"} \quad \text{Eq. (20)}$$

Furthermore, if (Ni=5), neighbour is a congestion node. Node is not allowed to participate in the election process. The equation is shown below:

$$\text{if } (N_i = 5) \text{ Than the Node is Congestion Node} \quad \text{Eq. (21)}$$

$$CH = Neighbor\ Node\ with\ \text{“}Maximum\ V_i\text{”} \quad \text{Eq. (22)}$$

CH will choose the neighbour with maximum Vi. The process continues to second stage where it is called stream position.

4.4.2.2 Stream Position Analysis Stage

At this stage, the CH maintains a trace file by monitoring the behaviour of the leaf node for each cycle of the transmission. Using its trace file, the stream position analysis will compute:

- The amount of data to be communicated,
- The payload of the packet,
- The amount of exact messages transmitted and
- The number of abnormal messages transmitted

The above features are calculated for every node at each cycle of its transmission. The flow chart for the Stream Position Analysis Stage is shown in Figure 4.11. In the flow chart, the process continues from the Cluster Head stage and is followed by the Stream Position stage. In the stream position stage, the cluster head will check the threshold value; if that value is less than equal to the threshold, it should omit the node. The equation is shown below:

$$if\ (CH\ checks\ the\ N_f \leq threshold)$$

$$Suspect = node\ i \quad \text{Eq. (23)}$$

Otherwise, the Cluster Head should choose that particular node for further processing, then classify the Suspect Node as Normal, and Calculate the distance of the node. Next, the algorithm will check if the packet size is greater than the threshold exceeded, then the process will correct the suspected node by reducing its (Vi) score and the node is not allowed to participate in the routing process. The equation is shown below:

if (Packet size > threshold exceeded) Classified Node as Attacker Eq. (24)

Moreover, if packet Size is less than the threshold, that means that node behaviour is normal and the node is allowed to participate in the process. The process will continue to the third stage, the CCA computation stage.

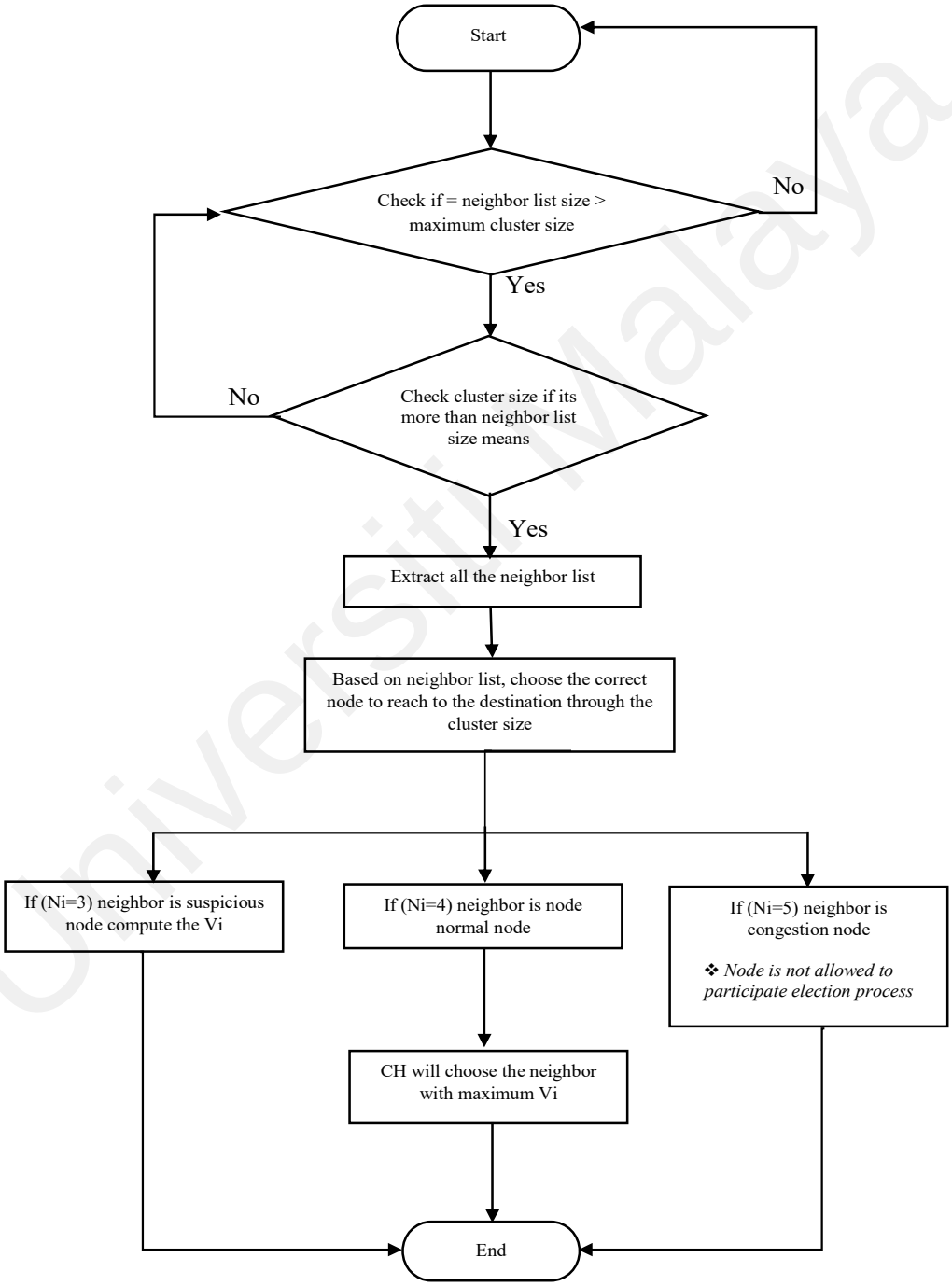

Figure 4.10: Flow Chart for Selection of Cluster Head Stage (SPPA)

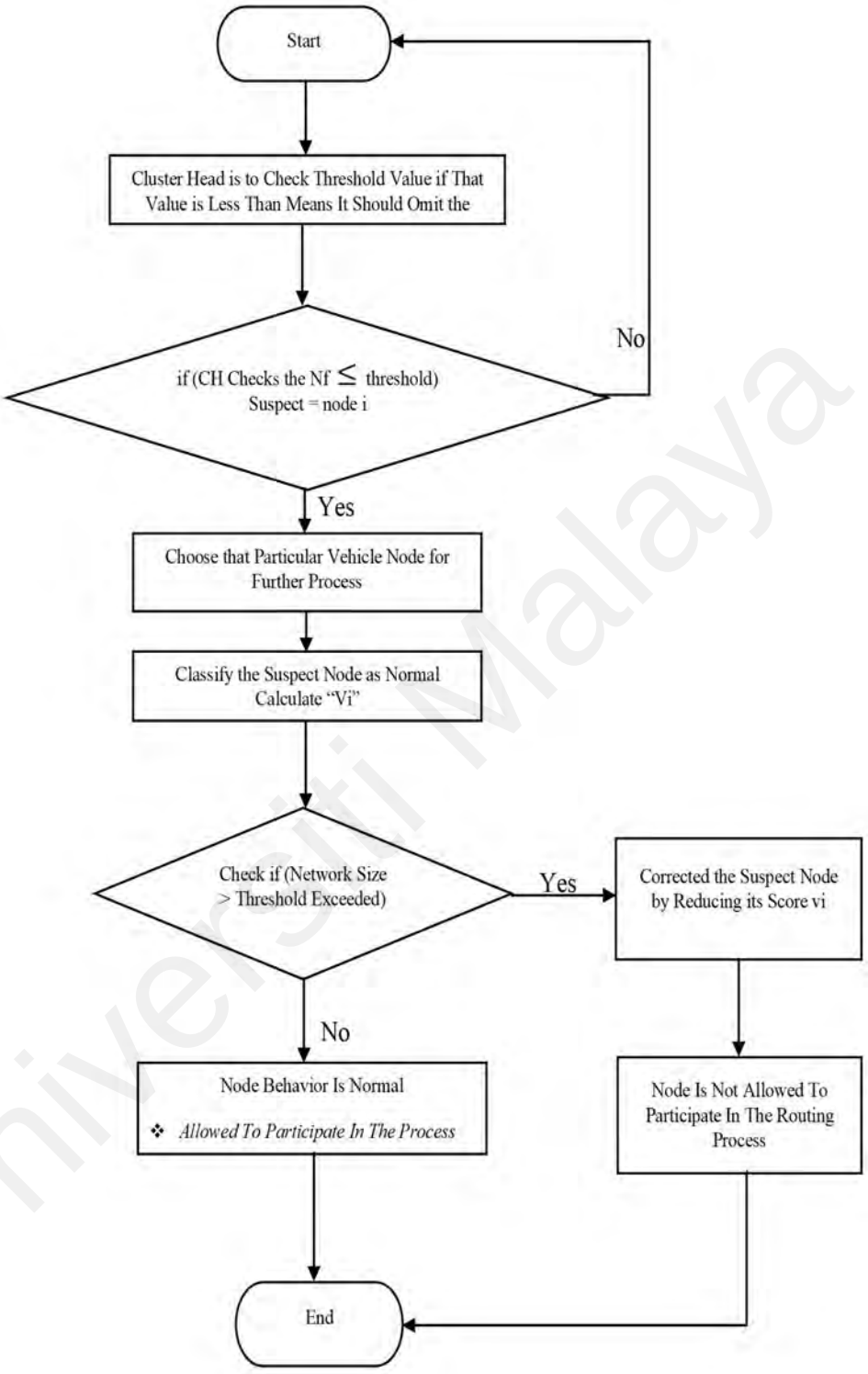

Figure 4.11: Flow Chart for Stream Position Analysis Stage (SPPA)

4.4.2.3 CCA Computation Stage

At this stage, the node parameters and node histories are considered for the process. The Conflict field means multiple cluster heads, meanwhile conflict data means repeated data, and the attack signature sample refers to previous history on the node or RSU. The CCA is calculated by computing the Conflict Field, Conflict Data, and Attack Signature Sample Rate (CCA) using the input factors such as:

- The number of packets or transmissions performed,
- The payload,
- The number of times a service is accessed (How many packets take as an input, for example a vehicle can access multiple safety and non-safety applications)
- The amount of exact access (for example, if the node is accessed by 100 packets, it will check one by one)

Using this above value, the DDoS attack detection is performed in the VANET environment. In this stage the process will compute the Conflict Field, Conflict Data and Attack Signature Sample Rate (CCA) of all the nodes to perform the detection. The flow chart for the CCA Computation Stage is shown in Figure 4.12. In the flow chart, the process is continuing from Stream Position and is followed by CCA computation. At first, the process will analyze the node behaviour (Vi). The "Vi" is focused on how many neighbours are available among the source nodes at that time to choose distances between the nodes. The process will calculate the conflict field using the equation as shown below:

$$CF = vi/n \qquad \text{Eq. (25)}$$

CF is Conflict Field, meanwhile vi is the Variable Score and n is the total number of nodes. Once calculated, the conflict field then calculates the conflict data. The equation is shown below:

$$CD = x/t \quad \text{Eq. (26)}$$

CD is Conflict Data, meanwhile x is the Distance of Nodes and t is Time. Once calculated, the conflict data then calculates the attack signature sample. The equation is shown below:

$$ASS = Size/DR \quad \text{Eq. (27)}$$

ASS is Attack Signature Sample, meanwhile Size is an abbreviation of Data Size and DR is Data Rate. Once calculated, the process will continue to the fourth stage called DDoS attack detection.

4.4.2.4 DDoS Attack Detection Stage

The detection is achieved by using the above models. It monitors the Stream of the node by tracing its incoming and outgoing packets and performs CCA calculation. Using the value, it calculates the legitimate weight of the node and comes to a conclusion, whether it is an intruder or normal node, and broadcasts the presence of the intruder and denies its service for the continued communication. The flow chart for the DDoS Attack Detection Stage is shown in Figure 4.13. In the flow chart, the process is continuing from CCA computation stage and is followed by DDoS attack detection. It checks for final confirmation among all the stages, then calculates the Stream Position Analysis (from Section 4.4.2.2) then only checks the CCA. If the condition is true, the Legitimate Weight LW is equal to CCA. The equation is shown below:

$$LW = CCA \quad \text{Eq. (28)}$$

If legitimate weight is equal to CCA, LW is checked to the Threshold Value. The equation is shown below:

$$LW > Th \quad \text{Eq. (29)}$$

LW means Legitimate Weight and Th is Threshold. If the legitimate weight is greater, the particular node is malicious otherwise the node is a normal node. The process will continue to the fifth stage called Attack Severity.

4.4.2.5 Attack Severity Stage

Finally, there is the attack severity stage. In this stage the algorithm will identify the attack as high impact or low impact, so that in the future, if the same type of attack happens, the VANET network will terminate the vehicle node. These features observe the characteristics of DDoS attack packets in vehicular communications in VANET. These features can be used to recognize and classify incoming attack packets in vehicular communications. Nonetheless, the structures are as follows:

Number of packets: Total number of packets from vehicle source to vehicle destination. During an attack, the attacker sends a large number of packets to the targeted vehicle.

Number of bytes: Total number of bytes sent from vehicle source to vehicle destination. Its intensifications when launching DDoS attack.

Average packet size: The ratio of number of bytes to number of packets. The equation as shown below:

$$NP * \frac{1}{(Te - Ts)} \quad \text{Eq. (30)}$$

NP is Number of Packets, meanwhile Te is End Packet Sent Time and Ts is Start Packet Sent Time. The algorithm calculates the packet rate per second from source to destination. It rises in attack time, and continues to calculate the First time-interval variance and final time-interval variance calculations. The equation is shown below:

$$\mathrm{t} = \frac{\sum t_i}{i} \quad \text{Eq. (31)}$$

where t is Time and i is Interval, it will calculate the time differences on vehicle first interval and time difference on vehicles final interval. Then calculate the time difference.

$$\frac{\sum(t_{n-}t)2}{n} \quad \text{Eq. (32)}$$

where t is Time. The final time calculated for one vehicle packet to another vehicle packet received at interval variance. Once completed, then the process will continue with vehicle packet start time-interval variance and vehicle packet end time-interval variance calculations. The equation is shown below:

$$\frac{\sum \boldsymbol{p_i}}{\boldsymbol{i}} - \frac{\sum \boldsymbol{t_i}}{\boldsymbol{i}} \quad \text{Eq. (33)}$$

$$\frac{\sum(\boldsymbol{p_{n-}}\ \boldsymbol{p})\boldsymbol{2}}{\boldsymbol{n}} - \frac{\sum(\boldsymbol{t_{n-}t})\boldsymbol{2}}{\boldsymbol{n}} \quad \text{Eq. (34)}$$

where p is Packet Size calculation, i is Initialized Interval and t is Time. Vehicle packet start time interval variance is calculated, followed by the Vehicle packet end time interval variance. Finally, if the destination packet size is equal to the source packet size, it is considered a low impact packet. The equation is shown below:

$$if(S = D) \quad \text{Eq. (35)}$$

where S is Source Sent Vehicle Packet and D is Destination Received Vehicle Packet. The packet is considered to be high impact if the packet size is different from the vehicle source packet size. The equation is shown below:

$$if(S! = D) \quad \text{Eq. (36)}$$

The flow chart for the **Attack Severity Stage** is shown in Figure 4.14. The explanation of the flow chart is given above.

Table 4.3: SPPA Abbreviations

Abbreviation	Meaning
N_L	Neighbor Lists
V_i	Variable Score (it's a boundary of 4 sides like north, east, west and south)
CH	Cluster Head
N_i	Neighbor initiate
N_f	Neighbor flow
P	Packet
CCA	Conflict Field, Conflict Data, and Attack Signature Sample Rate
I	Information
LW	Legitimate Weight
Th	Threshold
N_l	First neighbor
Node i	Initial node
Np	Number of Packets
Te	End Packet Sent Time
Ts	Start Packet Sent Time
SVPid	Vehicle Source Sent Packet Size with Vehicle ID
DVPid	Vehicle Destination Received Packet Size with Vehicle ID

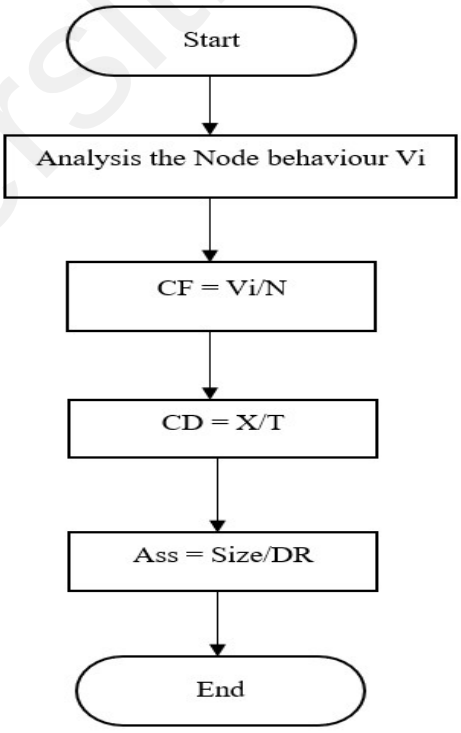

Figure 4.12: Flow Chart for CCA Computation Stage (SPPA)

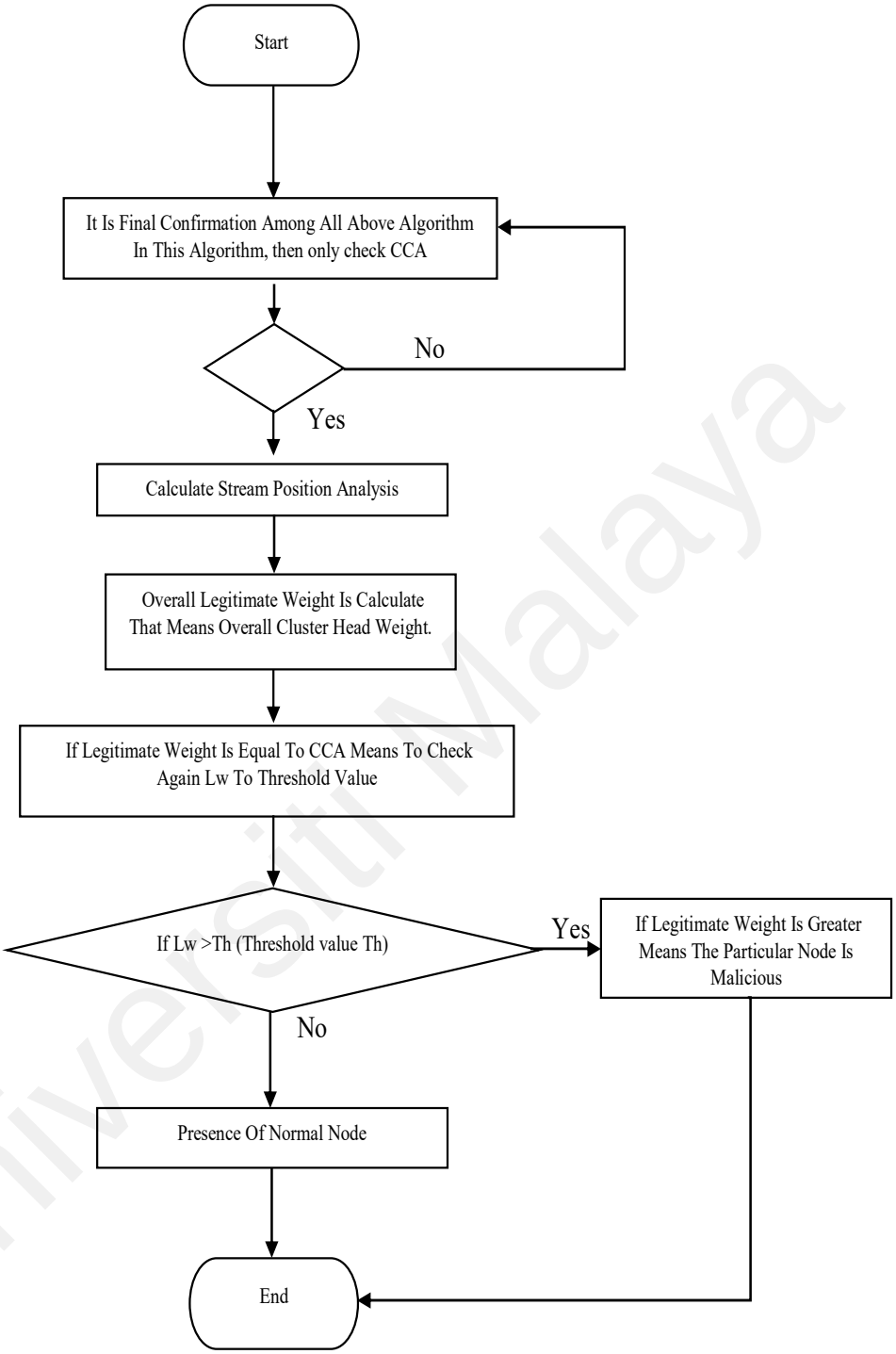

Figure 4.13: Flow Chart for DDoS Attack Detection Stage (SPPA)

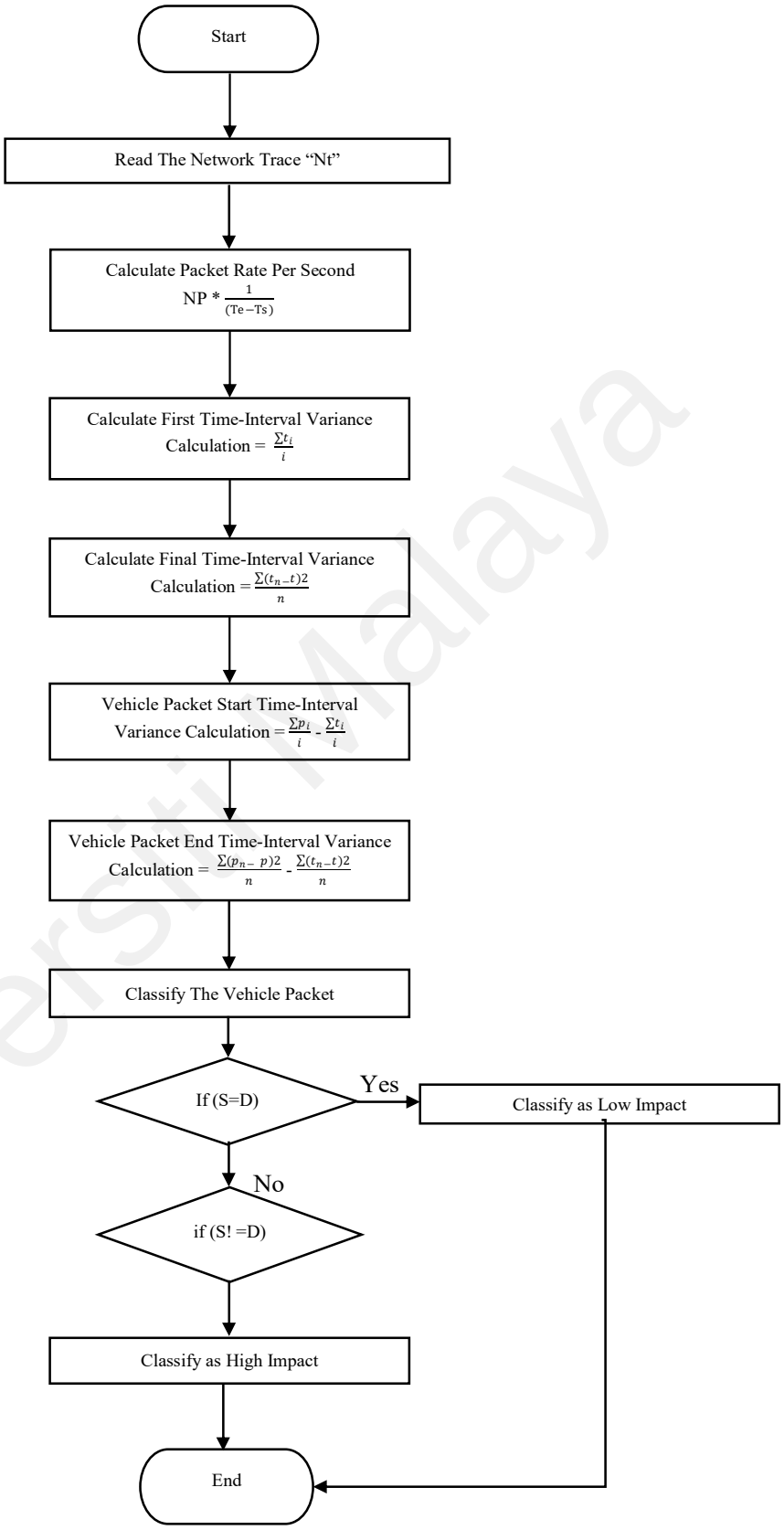

Figure 4.14: Flow Chart for Attack Severity Stage (SPPA)

4.6 Simulation Initial setup

In this section, we have showed the simulation initial setup in Ns2. This scenario is used to test and produce results for all the base models/methods in Chapter 5. There are several mobility generators developed for the simulation of vehicular scenarios which include but are not limited to FreeSim, VanetMobiSim, SUMO and MOVE. For this work I have used SUMO and we have used urban areas for simulation. Figure 4.15 shows the standard format of the OSM file that is imported to SUMO

4.6.1 Proposed Model

In order to get accurate environments in Ns2, we are simulate the traffic area in Bangsar, Kuala Lumpur. The actual map is shown in Figure 4.17. Figure 4.16 is an Open Street Map (OSM) file that is imported into SUMO using a real-world format. In the simulation environment the vehicle movements are not constrained. The vehicle node can enter and exit the main road from all 4 directions. The number of vehicle nodes are randomly created in the 4-junction road. About 150 vehicle nodes are used for the simulation.

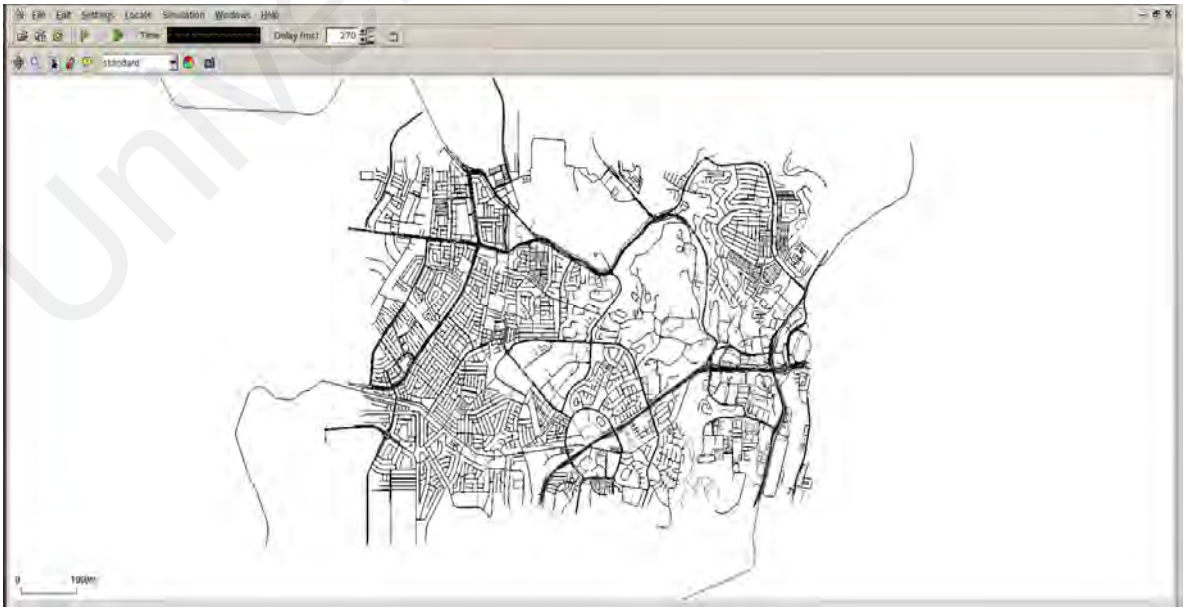

Figure 4.15 OSM File Imported into SUMO Standard Format

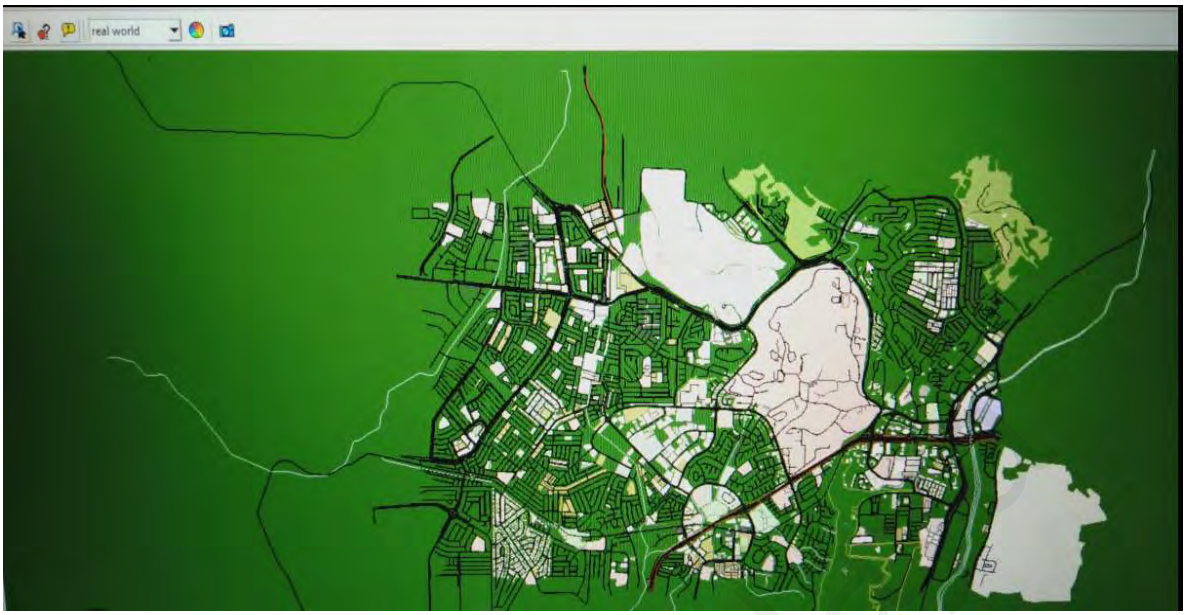

Figure 4.16 OSM File Imported into SUMO Real World Format

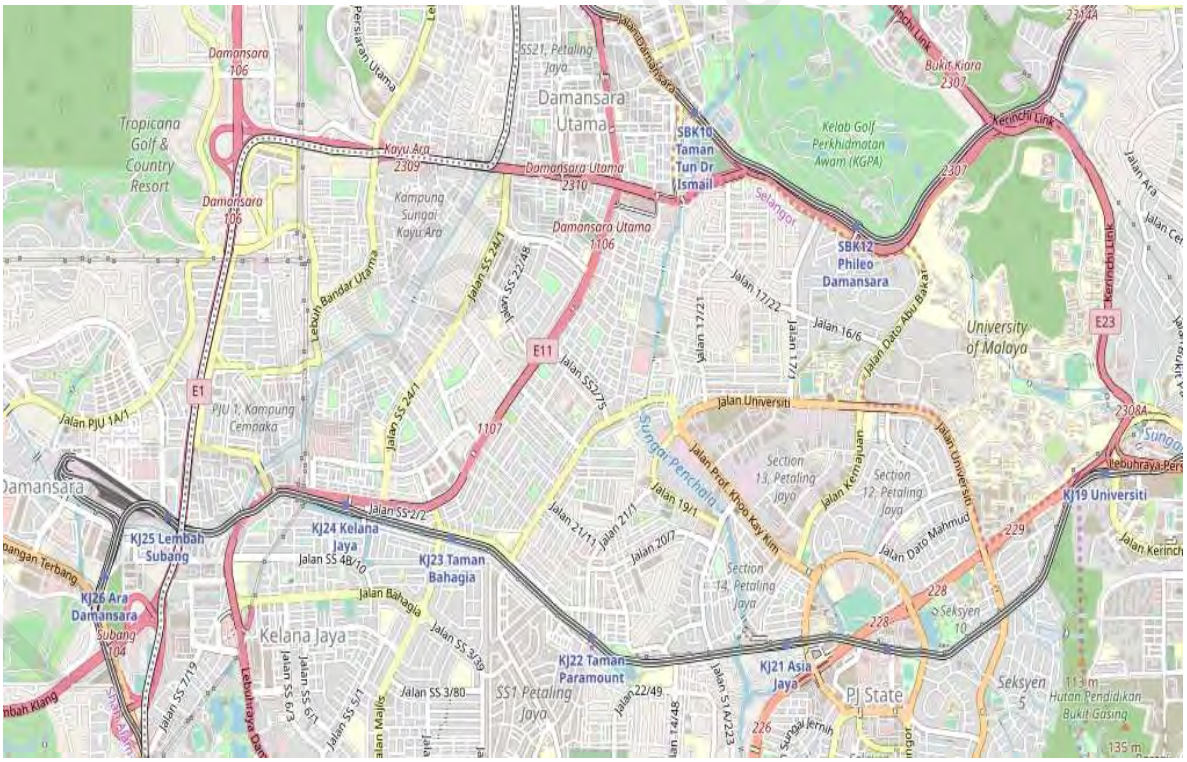

Figure 4.17: Extracted Road Map of Bangsar, Kuala Lumpur From OSM Database

Seven performance metrics have been measured for the proposed model: Packet Delivery Ratio (PDR), End to End Delay, Throughput, Routing Overhead (RO), Attack Detection Rate, Attack Detection Time and False Classification Ratio (Saritha et al., 2017) (Shah et

al., 2018). The seven-performance metrics are divided into two categories; the first is DDoS metrics and the second comprises network metrics. The main aim of the performance metrics is to evaluate the performance of the MVSA and SPPA model to detect the DDoS attack in vehicular communication in VANET (Sharma & Sharma, 2017). We are using the latest dataset for this work and it is called "i-VANET Dataset for Vehicular Communication". The dataset is available in the following link https://www.bits-pilani.ac.in/pilani/ProjectiVANETs/DatasetforVehicularCommunication.

4.7 Conclusion

In this chapter, the development of the proposed Multi Variant Stream Analysis and Stream Position Performance Analysis model for detection of DDoS attacks in V2V communication has been presented. The methods will answer and solve the few of the identified challenges from Chapter 3. The complete methodology of the study along with an explanation of each model and stages has been given in consequent sections of this chapter. The algorithm for each stage was also explained in detail. The first model will solve the packet classification issue and will perform the marking on vehicle packets**.** Finally, the second model will improve the detection time and classify the attacker as high impact or low impact. Besides that, the theoretical viewpoints from previous studies have been applied to achieve the solutions for the problems that occurred. In the following chapter, comprehensive and detailed explanation of the execution procedure using network simulations will be presented. Also, a detailed and comprehensive explanation of the implementation procedure using network simulations will be presented, followed by an explanation of results and validation results.

CHAPTER 5: RESULTS AND DISCUSSION

5.1 Introduction

In this chapter, the experiment and investigation will be described with a discussion of the results. The Ns-2 and Ns-2 architectures will be explained in detail. In order to bring out the whole idea of this study, some important knowledge and skills are needed. In the following sections, the related research and the parameters of both models will be discussed. Besides that, the experimental results for the existing model and our proposed MVSA and SPPA models will be discussed. Moreover, this chapter also present on the result validation. Finally, the vehicular node and performance evaluation metrics will be covered in detail.

5.2 Network Simulation (Ns-2)

Ns-2 or Network Simulator Generation 2 was introduced in 1989 and established as a part of the Virtual Internet Testbed (VINT). It is currently maintained by volunteers throughout the world. Ns-2 is freely distributed open source software for NT research. For academic purposes, it is used for designing protocols and analyzing traffic. Most UNIX and UNIX like systems and windows platforms are supported by the Ns-2 Simulator.

Ns-2 delivers extensive support for replication of the Transmission Control Protocol (TCP), multicast and routing protocols over wireless and wired networks. In addition, it comprises 2 simulation tools as well as all frequently used IP protocols. Ns2 entirely pretends to be a layered network from the physical radio transmission channel to high-level requests or applications. Besides that, the Network Animator (Nam) is a castoff for imagining simulations. The Ns2 is an object-oriented simulator written in OTCL and C++. C++ is used for the formation of objects for speed and competence (Zhibin, 2007). However, OTCL is a

front-end platform for setting up objects and planning actions for convenience of use. Normally, the simulator will support a class hierarchy in C++ and a comparable class hierarchy inside the OTCL interpreter. Finally, one-to-one communication among the classes in the hierarchy is interpreted in the compiled hierarchy. C++ is appropriate for applications that consume high speed requests while OTCL is appropriate for plans and formations that demand speedy modifications (Zhibin, 2007).

The Ns2 is extremely extensible. Most of the time it not only supports most common IP protocols, but it permits the users to implement or extend their protocols. Besides that, the newest Ns2 supports two ad hoc routing protocols, together with Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR). It also offers important trace functionalities, which are critical in this research, as well as numerous information essential for analysis. The occupied source code of Ns2 can be copied and compiled for numerous platforms such as Cygwin, Windows and UNIX. The CBR is in a manual starting position to give the same scenario file since there will be difficult nodes and at different times nodes will have high mobility and speed, etc. The initial stage is used to store used movement joints and at different times for each movement, a random value generator is used. The node motion generator/indep-utils included/CMU-scene-zen/setdest/directory is available under the EXE file name "setdest." This file runs some logic to create the file in context.

5.2.1 NS-2 Architecture

The Ns-2 is written in C++ but the front-end interpreter uses Object Tool Common Language (OTCL). Ns-2 is an OTCL translator that takes an OTCL script as input and creates a trace file as output. Ns-2 can be designed according to the needs and requirements or can be

modified through the existing protocol inside the Ns-2. The Ns-2 is normally used in networking or wireless projects. Apart from that, Ns-2 will be used to simulate TCP/IP, multicast and routing protocols in wireless and wired networks. Ns-2 is valuable to new advanced network protocols. Furthermore, Ns-2 is capable of running huge experiments and primarily simulations. Also, the Ns-2 is more reliable in Linux, Windows and Macintosh environments. Figure 5.1 shows the architecture of Ns-2 (Zhibin, 2007).

In the following, the study will discuss OTCL and TCL in more detail. OTCL is one of the scripting interfaces used in Ns-2. OTCL is also called Object-Oriented TLS. The classes of OTCL mainly support and delimit the method inside OTCL. However, TLC is mainly used for the scripting language. There is another way to access the library function using C compared to the other simulator. TCL is much easier interface with its functionality. The connection between OTCL and TCL is parallel to C and C++. OTCL was created by David Wetherill (Zhibin, 2007).

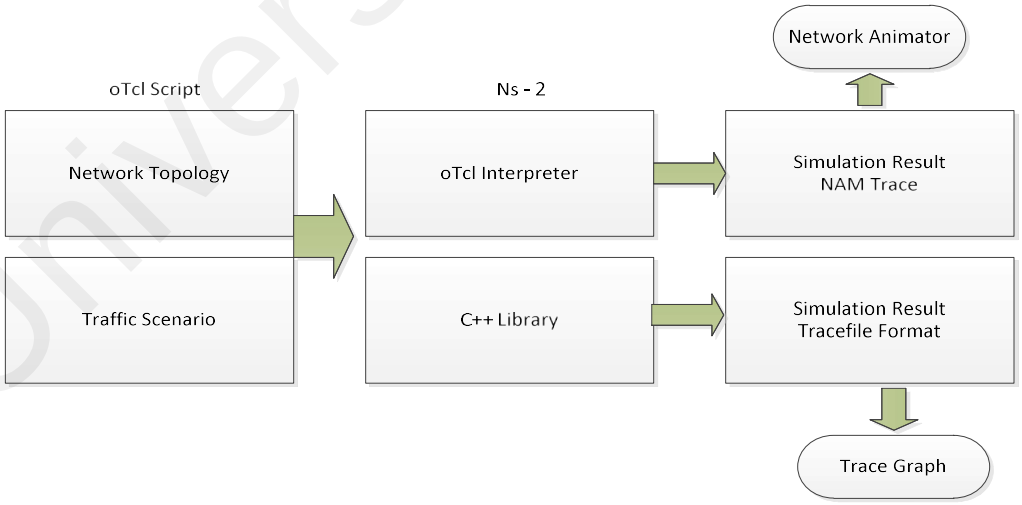

Figure 5.1: Ns2 Network Architecture

Source: *Adapted from Zhibin, W. (2007). Network Simulator 2 for Wireless. New Jersey: WINLAB, Rutgers University.*

5.2.2 Vehicular Node Components

The vehicular node components are normally used for Ns-2 simulations. The researcher creates one network topology in Ns-2 for all the three models. The mobile node plays an important role in the Ns-2. The vehicular node components are mainly used to setup the MAC type, traffic type and others (Bordbar & Anane, 2005).

Besides that, some of the important vehicle node components will be discussed. A link layer is used in the ARP module and acts similarly to an LAN. The ARP module will carry one packet to the same target destinations. The MAC layer is normally used for the IEEE 802.11 protocol. The MAC layer will acknowledge all the unicast packets in the vehicular and mobile nodes, whereas network interface (PHY) will support the DSSS parameter and update the energy starting with reception and transmission. Nevertheless, the antenna is another vehicular node component which is normally used together with the Omni directional antenna and others. The radio propagation model will be used via two methods. The first method is two-ray ground reflection which is used for long distances. The second method is known as friss-space attenuation and is used for near distances. In these studies, there are some parameters for declaration. However, the declaration method is for experimental purposes. The method shown about the channel type, routing protocol, network interface type, antenna model, number of vehicular nodes, time of simulation, MAC type and so on.

5.3 Simulation scenario

The method has been validated for its efficiency by sometimes maintaining logs. By using the network trace, the performance of the method for DDoS attack detection was measured. In order to assess the performance, a 4-junction road was considered. In the simulation, the

vehicle can initiate a request for its attentive data. However, in the simulation, they were set 150 vehicle nodes located randomly within the margins. Nevertheless, the vehicle can travel in any direction on the 4-junction road. The simulation was executed for 200 Seconds (Hafeez et al., 2010). Table 5.1 shows the simulation configuration and parameters for evaluation. However, the mentioned parameters were used in Ns2 to generate a simulation of a detected DDoS attack.

This research has used the AODV routing protocol (Sailaja et al., 2018, Raju et al., 2013). There are four-junction roads, with two lanes in each direction. As shown in Figure 5.2, there are four crossing junctions through which vehicles may cross each other on the road. In the scenario depicted in the figure, car D is attacked by cars A, C, and E. Car D is trying to communicate with car G because car D wants to inform it about an accident in front involving a nearby vehicle. But the communication is cannot go through because car D is under attack and is overloaded with messages from cars A, C and E. This is where our proposed model will work to detect the DDoS attack. The result of the simulation is shown in the NAM file, including the trace file routing parameter gained.

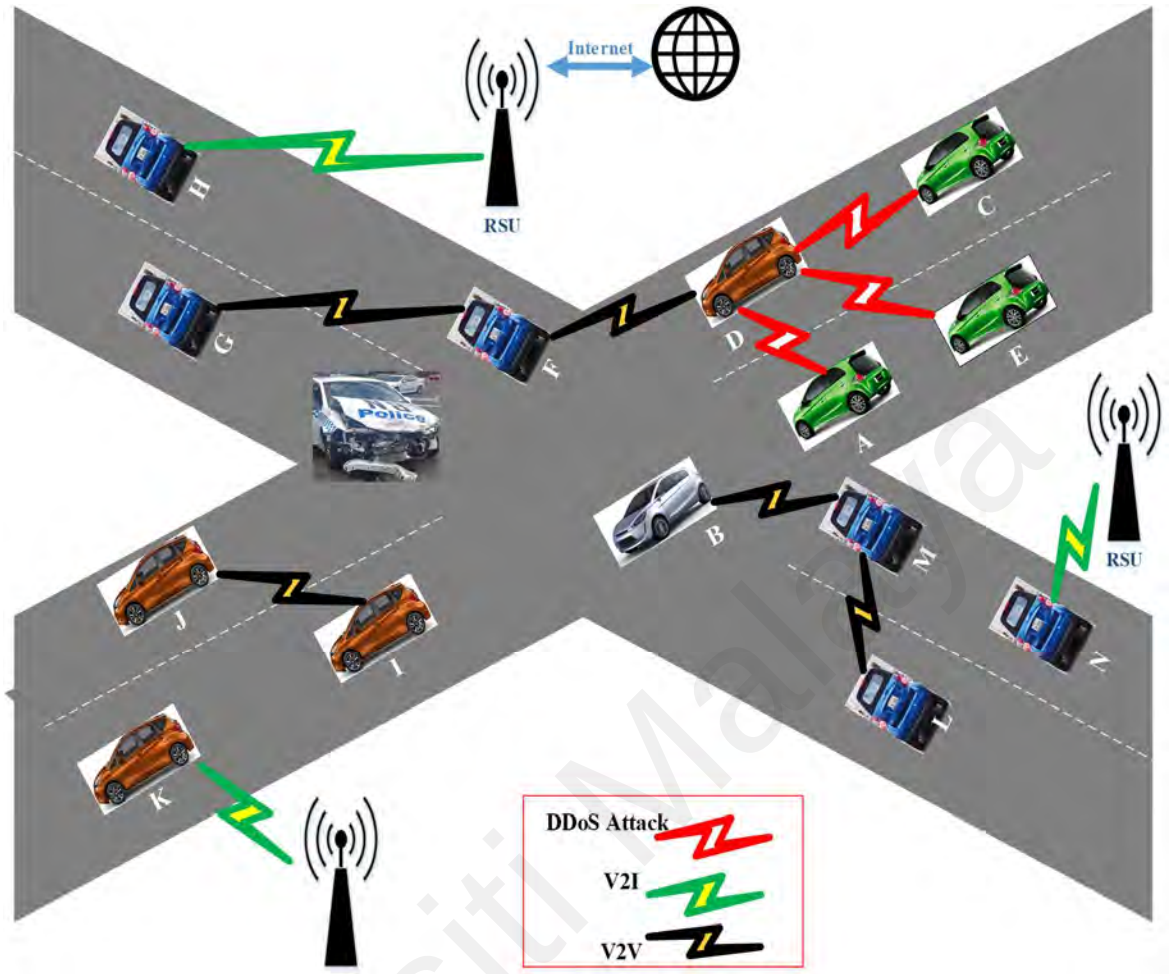

Figure 5.2: Simulation Scenario

5.3.1 Simulation Parameter

However, the efficiency of this method is that it is able to detect the attack in the minimum time, so that communication can continue smoothly. The outcome of this method is shown in the simulation results. DDoS attack detection has been realized in network simulator version Ns2.34 under various scenarios. The behaviour of the suggested approaches is analyzed with a variety of simulation parameters. A vehicle node can accurately convey the message to the other vehicle or hubs that exist in its communication range. If a vehicle node needs to speak with a centre or base station that is not directly inside its communication run, then it utilizes transitional hubs as switches (Sharma & Sharma, 2017). In a portability

display, the energy of a vehicle node from one area to another can be empowered using the catchphrase "setdest" in the Tool Command Language (TCL). Vehicle nodes are arranged with the segments of the channel, organizing interface, radio propagation and Medium Access Control (MAC) conventions.

Table 5.1: Simulation Configuration

PARAMETER	VALUE
Platform	Ns2.34
Topology Size	1000m * 1000m
Packet Size	512 Bytes
Simulation Time	200 Sec
Node Speed	30 m/s
Number of Nodes	15, 30, 45, 60, 75, 90, 105, 120, 135, 150
RSU	3
MAC Layer	IEEE 802.11p
Antenna Model	Omni-directional Antenna
Data Transmission Range	20 Mbps
Bandwidth	2 Mbps
Mobility Model	Random Way-Point

In dominant topology, the neighbours of every vehicle node substitute with the specific vehicle nodes for the area. The developments of portable vehicle nodes are bound to a region of 1000m * 1000m. In the work we have used average node's speed (30 m/s), this is the average vehicle speed based on the existing research paper simulation (Vipin & Chhillar, 2018). Furthermore, in this work I have used random mobility model for both simulations. This is because of in the road, the vehicle nodes are move randomly and its freely move without any restrictions. In more precise, the speed, destination and direction will choose randomly. Most of the DDoS attack detection simulations are used random mobility model to get more precise outcomes. Currently most of the simulation studies are used random mobility model. The random mobility model was firstly used by Johnson & Malthz in the

year 1996 (Johnson & Maltz, 1996). Information transmission is built up between nodes operating with CBR traffic movement. Our proposed model is compared with three existing models; they are:

- *The DDOS Attack Detection and Prevention in VANET by Group Controlled Analysis Model (Vipin & Chhillar, 2018)*
- *Sentinel: Defense Mechanism Against DDoS Flooding Attacks in Software Defined Vehicular Networks (SDM) (Biasi et al., 2018)*
- *A Novel Security Approach for Data Flow and Data Pattern Analysis to Mitigate DDoS attacks in VANETs (DF) (Kaur & Mahajan, 2015).*

The simulation configuration is shown in the Table 5.1. Seven performance metrics have been measured for the proposed model:

- *Attack Detection Time*
- *Attack Detection Rate,*
- *Packet Delivery Ratio (PDR),*
- *End to End Delay,*
- *Throughput,*
- *Routing Overhead (RO),*
- *False Classification Ratio (Saritha et al., 2017, Shah et al., 2018).*

5.3.2 Performance Metrics

These performance metrics are divided into two categories. The first is DDoS metrics which consist of Attack Detection Time, Attack Detection Rate and False Classification Ratio (Saritha et al., 2017, Shah et al., 2018). The second category consists of network metrics, such as Throughput, End to End Delay, Packet Delivery Ratio and Routing Overhead. Both categories of metrics need to be evaluated so that we can get the accurate results for the proposed DDoS attack detection model.

i. Attack Detection Time - Before we calculate the attack detection time, we need to identify the malicious nodes first. The identification of malicious nodes is done in our proposed models and it will measure how fast the attack is detected using proposed models. Malicious vehicles send interfering messages to drop communications between legitimate vehicles. Apart from that, malicious vehicles can corrupt or capture data from other vehicles when it is an intermediate node. In the VANET environment, vehicles are able to know about the velocity and location of other vehicles (Fotohi et al., 2016). The result is obtained from the following formula where Detection time is the total time taken to detect the misbehaving nodes in the route from source to destination (Sangulagi et al., 2013). The equation is shown in Eq. (37). DT means Detection Time, meanwhile PL is Path Length which is how far the node travels, and TT is Time Taken for malicious packets to travel from source to destination.

$$DT = (PL/TT) \quad \text{Eq. (37)}$$

ii. Attack Detection Rate - It is applied to estimate the position of a vehicle in VANET environments by implementing the routing scheme. Attack detection rate specifies the percentage of how regularly the system effectively distinguishes the attacks from the

initial vehicle point to the destination or ending, and the ratio of the number of nodes are properly recognized by the VANET network to be dropped under an attack (Pavan et al., 2019). The result is obtained from the following formula:

$$Attack\ Detection\ Rate\ = (Total\ Number\ of\ Attacks\ / \ Total\ Number\ of\ Detected\ Attacks)\ * 100\% \quad \text{Eq. (38)}$$

iii. False Classification Ratio - this is applied to measure detection classification accuracy and how often it wrongly classifies genuine nodes as malicious. The false classification has been performed either by classifying the true node as false, or the false node as true. So, by computing both, the false classification ratio can be calculated. Moreover, the TP is the number of packets delivered from source to destination which is related to the throughput and FP is a number of dropped packets or genuine nodes classified as malicious, which is related to latency. The result is obtained from the following formula:

$$False\ Classification\ Ratio\ = \frac{\psi TP + \psi FP}{Total\ number\ of\ nodes} * 100 \quad \text{Eq. (39)}$$

Here ψTP – True positive and ψFP- False Positive.

iv. Throughput - Throughput is measured based on the number of bytes being sent from a vehicle's source node towards the vehicle's destination and the number of bytes being received at the vehicle's destination at any point in time (Alheeti et al., 2017). Throughput is measured in Kilobits per second (Kbps). For any protocol to prove its efficiency, it should achieve higher throughput. The results arise from the following formula:

$$Throughput\ (byte\ persecond)\ =\ Sum\ (Number\ of\ Successful\ Vehicular\ Packets)\ * (Average\ Packet\ Size)\ / \ Total\ Time\ sent\ in\ delivering\ that\ amount\ of\ data\ send\ to\ vehicle\ destination \quad \text{Eq. (40)}$$

v. End to End Delay - End to End Delay denotes the time taken for a vehicle's message to be conveyed across a VANET network from a vehicle's source to its destination. The message we send is really a critical message and should be reached on time. If it is delayed, then any unwanted disaster can happen. From a vehicular perspective, delay is determined by the message's responsiveness to other vehicles or drivers. The same can be measured based on the number of packets received at the destination at any point in time. The result is obtained from the following formula:

$$End\ to\ End\ Delay\ = (Time\ \ the\ packet\ reaches\ the\ vehicle\ destination - time\ of\ the\ packet\ generated\ by\ the\ vehicle\ sources) \quad \text{Eq. (41)}$$

vi. Packet Delivery Ratio – PDR depends on the performance of the routing protocol in the VANET network. There are some important parameters to measure the packet delivery ratio, for example, structure of the vehicular to vehicular communication in the VANET network, packet size, transmission range, and the number of vehicular nodes. The packet delivery ratio can be calculated by dividing the number of vehicle packets sent from the source by the number of vehicular packets received at the destination. The higher the vehicle packet delivery ratio, the better the performance. By taking this performance metric, a comparison between the routing mechanism and the current mechanism on the same metric can be carried out to evaluate the performance of MVSA and SPPA models with existing methods. The result is obtained from the following formula:

$$PDR\ = (\Sigma\ Average\ Number\ of\ Packet\ Received\ by\ Vehicle\ destination\ /\ \Sigma\ Total\ Number\ of\ Packets\ Generated\ by\ Vehicle\ Source)\ *\ 100 \quad \text{Eq. (42)}$$

vii. Routing Overhead (RO) - This is the number of routing packets used because of frequent link breakages that lead to regular path failures and route discoveries. The routing overhead increases with the number of vehicle nodes, since the control messages become enormous in VANET networks as they contain the whole neighbour vehicle list. The vehicle routing packet will retain the updated information about the network routes and the algorithm of routing will produce small size vehicle packets named routing packets. For example, to check whether a neighbouring vehicle is active or not by using a "HELLO" packet. Normally, the routing will not carry and application content comparable to the date packet will. Most of the time the network bandwidth needs to be shared by data packets and routing. The overheads in the VANET network are based on routing packets and is called routing overhead. According to research, a good routing protocol would sustain a lower routing overhead. By taking this performance metric, the comparison between the routing mechanism and the current mechanism or method on the same metric can be carried out to evaluate the performance of MVSA and SPPA model against the existing methods. The results can be obtained from the following formula:

$$RO = Total\ Number\ of\ the\ Routing\ Packets\ \ / \\ Total\ Number\ of\ Data\ Packets\ Received\ from\ Source\ Vehicle \quad \text{Eq. (43)}$$

5.4 Validation Techniques

Result validation is regularly witnessed as the most challenging phase of finishing the study or research, that are not the way. However, we must to know what we want to do with the data that we have collected, and exactly how to explain the outcomes. The program that is intended for statistical analysis be able to make the process as easy as conceivable. Currently

there are a number of statistical tools offered on the market to take out statistical analysis of results. In this part we are going to discuss the six best packages suitable for result validation.

i) **SPSS** (Statistical Package for the Social Sciences) is most commonly used IT and non-IT related research. Moreover, it recommends the capability to clearly compile descriptive statistics, non-parametric and parametric analyses, and graphical descriptions of results across the graphical user interface (GUI). It includes the choice to generate scripts to computerize analysis or produce the more complex statistical processing. The SPSS software is licensed software.

ii) **R** (R Foundation for Statistical Computing) it's a open source statistical software bundle or package that is commonly used in IT and human behaviour research. Moreover, the Toolboxes (effectively plugins) are accessible for a huge variety of applications, which can make easier and simpler data managing or results. Although R is a very dominant piece of software, it also consists of learning curve, demanding a specific degree of experience on coding.

iii) **MATLAB** (MATrix LABoratory) it's also a programming language and analytical or logical platform that is commonly applied by scientists and engineers. Furthermore, the R is a learning way on steep, and we needed to build our own source code at some point. Sometime the MATLAB can be challenging whenever use novices, it suggests a huge amount of elasticity in terms of what we choose to do – if we can code it.

iv) **SAS** (Statistical Analysis Software) is another statistical analysis program that suggests alternatives to use any of the GUI, or to produce our own scripts for complex analyses. It's a premium mixture that is commonly used in healthcare, IT research and business. It is conceivable to execute complex analyses and make publication-worthy charts and graphs, even though the coding sometime be more challenging and sometime some user need modification for individuals not used to this style.

v) **GraphPad Prism** it's another exceptional software mainly used surrounded by statistics related to IT, Healthcare and proposes a variety of abilities that usually used among numerous fields. Likely to SPSS, the scripting choices are accessible to computerize analyses, or perform more complicated statistical methods or calculations, in this program most of the work can be done with the GUI.

vi) **Minitab** is another premium program that offers a selection of both simple and complex statistical tools for analysis of data. Like GraphPad Prism, the instruction can be performed via scripted commands or GUI, getting it available to beginners as well as users considering performing more complicated analyses.

There is a range of different software tools available, and each offer something slightly different to the user – what we choose will depend on a range of factors, including our research question, knowledge of statistics, and experience of coding. To validate the results on this research, Minitab version 18 has been chosen. The analysis includes descriptive statistics, and Anova test supported by Tukey comparison test to detect significant differences among 5 models. Minitab is used because it will generate robust results. Minitab has a user friendly and intuitive interface. Moreover, it has a familiar worksheet look and

feel. Additionally, it identifies distributions, correlations, outliers, missing values and more, then easily illustrates the findings with a variety of graphs, charts and predictive analytics.

5.5 Simulation Results Discussion

In this section we will discuss the outcomes from the 2 models and 7 performance metrics with the aid of graphs. In the proposed models results all the 7-performance metrics are started with zero for x- and y- axis. Furthermore, the graph's axis is labeled consistently and informatively. This is to shows more precise results for understanding purpose. Each and every value in the graph is very important to show the changes based on the simulation results and it will show how accurate is the MVSA and SPPA DDoS attack detection model are working. In the proposed model's simulation, I have used random false data injection. The main purpose of the random false data injection is to find any DDoS attack vector that can result in a wrong estimation of state variables. According to author (Diaz & Sanchez, 2016) when we simulate DDoS attack detection environment it's better to use random false data injection to get the more accurate outcomes. In the proposed work we only simulate safety application traffic. The safety application is really important in VANET, if the important message is received late then it's pointless.

5.5.1 Attack Detection Time

Normally the detection time is measured based on the time at which the vehicle packet has been sent from the origin and the time when it has been delivered at the destination vehicle. Figure 5.3 demonstrates the Attack Detection Time as a function of time when the baseline methods (MVSA & SPPA) are compared with the GAC method, SDM method and DF

method. Its shows the qualified examination of Attack Detection Time of the planned structure with the remaining, based on the values given in Figure 5.3.

The detection time of GAC is inferior compared to all other approaches because this approach is only focused on throughput, packet drop ratio and packet delivery ratio for the VANET network. GAC did not focus on detection time, and overall performance. The attack detection time for GAC is 0.4 seconds. Besides that, the SDM method has improved its detection time to about 0.12 seconds. It has improved by 0.28 seconds with the existing GAC method. Moreover, the DF method can detect the attack within 0.25 seconds. It considers slightly higher at 0.13 second compare with SDM method. The first proposed MVSA model is able to detect the attack in 0.1 second and its show better improvement from all the 3 existing methods. MVSA model is improve 0.3 second from existing GAC method. Whereas, the MVSA model improve 0.02 seconds from SDM model and its improve 0.15 seconds from DF method. Finally, the proposed second model SPPA has slightly improved the detection time at 0.08 seconds and it shows much better improvement from all the 3 existing methods. SPPA model is improve 0.32 seconds from existing GAC method. Whereas, the SPPA model improve 0.04 seconds from SDM model and its improve 0.17 seconds from DF method. In conclusion the SPPA model recode the lowest timing with 0.08 seconds to detect the DDoS attack in vehicular communication in VANET environment.

This detection time for the SPPA model constantly outpaces baseline methods. However, this model uses Conflict Field, Conflict Data, and Attack Signature Sample Rate (CCA) to detect a DDoS attack and it took a minimum time to detect the attacks compared to other methods. The performance of this model improves with time. The safety related message needs to be received on time without any delay, and to avoid any delays the SPPA model is

implemented to detect the attack within a minimum time frame. According to the analysis graph, the detection time is clearly within the minimum time. In the Figure 5.3. we can see that the graph is spike when the number of nodes is 15, the main reason is the node are not able to perform well its due to lack of communication among the nodes (Kumar & Shina, 2014).

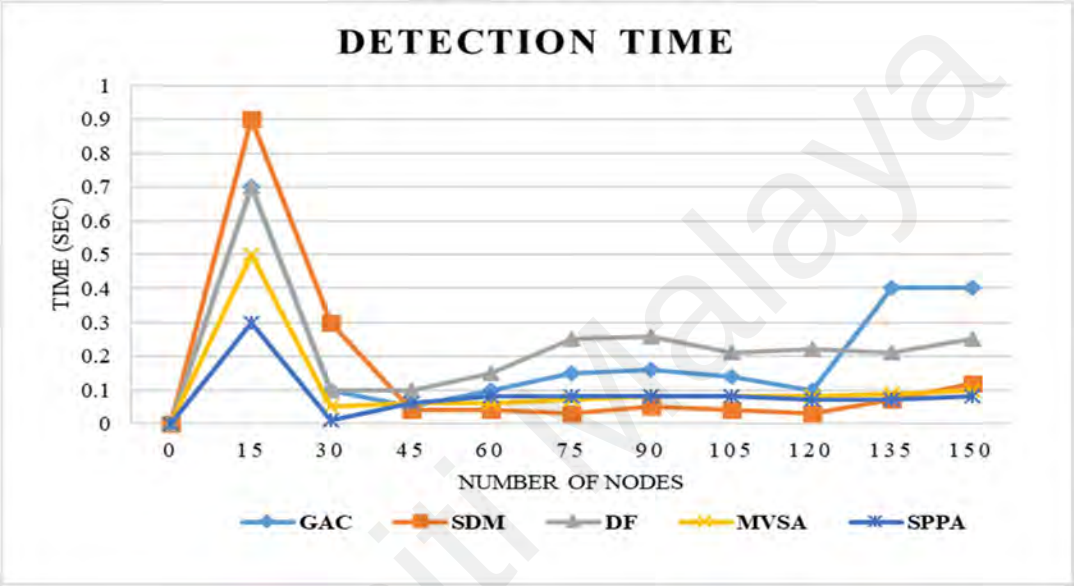

Figure 5.3: Attack Detection Time Analysis

5.5.1.1 Validation Results for Attack Detection Time

In the case of attack detection time, results are presented in Table 5.2 below. This ANOVA model is reliable as supported by the residual plot in Figure 5.4 below and it shows that the distribution of the probability plot of the five models is quite normal and there are no significant outliers. Further test was conducted to detect the differences among the models by using the 'Tukey pairwise comparison' technique as presented in Table 5.4. The results indicate that significant differences are registered between MVSA & DF (p=0.006); SPPA & DF (p= 0.000); MVSA & GAC (p= 0.006); SPPA & GAC (p= 0.000) at the 95%

confidence level. Meanwhile, SPPA & SDM also shows a significant difference (p= 0.067) at the 90% confidence level.

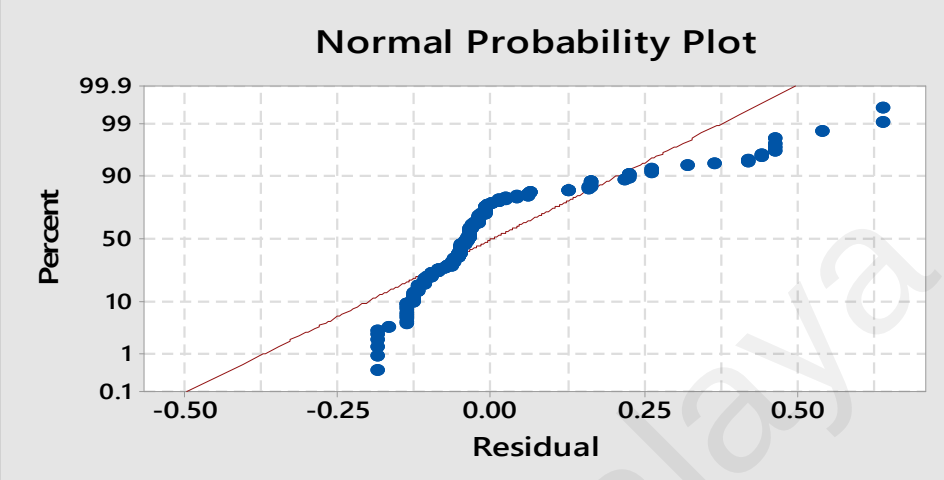

Figure 5.4: Residual Plots for Attack Detection Time

Table 5.2: Tukey Pairwise Comparison for Attack Detection Time

Difference of Levels	Difference of Means	SE of Difference	95% CI	T-Value	Adjusted P-Value
GAC - DF	0.0000	0.0447	(-0.1235, 0.1235)	0.00	1.000
MVSA - DF	-0.1563	0.0447	(-0.2798, -0.0328)	-3.50	**0.006**
SDM - DF	-0.0783	0.0447	(-0.2019, 0.0452)	-1.75	0.405
SPPA - DF	-0.1966	0.0447	(-0.3201, -0.0730)	-4.40	**0.000**
MVSA - GAC	-0.1563	0.0447	(-0.2798, -0.0328)	-3.50	**0.006**
SDM - GAC	-0.0783	0.0447	(-0.2019, 0.0452)	-1.75	0.405
SPPA - GAC	-0.1966	0.0447	(-0.3201, -0.0730)	-4.40	**0.000**
SDM - MVSA	0.0780	0.0447	(-0.0456, 0.2015)	1.75	0.410
SPPA - MVSA	-0.0403	0.0447	(-0.1638, 0.0833)	-0.90	0.896
SPPA - SDM	-0.1182	0.0447	(-0.2418, 0.0053)	-2.65	**0.067**

Note: - F-Test =8.02, P Value = 0.000

5.5.2 Attack Detection Rate

The ADR is the percentage at which the DDoS attacks are detected in vehicular communications in VANET networks. However, when the vehicle node size rises, the percentage of the DDoS attack rises, which leads to the intensification in the attack detection rate. The DDoS attacks are detected without difficulty in an appropriate manner. Figure 5.5 demonstrates the ADR as a function of detection rate when the baseline methods (MVSA & SPPA) are compared with the GAC method, SDM method and DF. It shows the qualified examination of the Attack Detection Rate of the planned structure with the remaining, based on the values given in Figure 5.5.

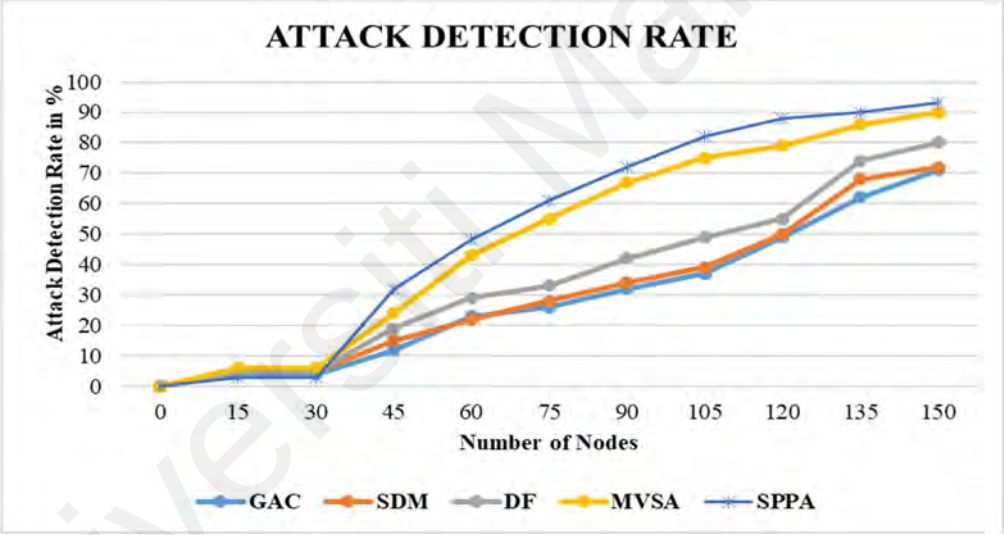

Figure 5.5: Attack Detection Rate

The SDM method has an average increase in Detection Rate of 1% over the existing GAC method. Besides that, the DF method increased its detection rate with an average of 8% over the SDM method. In addition, the first proposed MVSA model increased its detection rate with an average of 10% over the DF method. Finally, the proposed second model SPPA has improved its detection rate by an average of 3% over the MVSA model.

In conclusion, the proposed SPPA model outperforms all other models in terms of detection rate. Moreover, when the detection rate for both existing and proposed algorithms are calculated, the proposed model provides a high detection rate with an average of 22% over the existing GAC method. Besides that, when we compare with SDM method, it yields 21% and the DF method offers a 13% detection rate when compared to the SPPA model. According to the analysis graph, the detection rate is clearly improved to 93% compared to other existing methods.

5.5.2.1 Validation Results for Attack Detection Rate

In the case of detection rate, results are presented in Table 5.3 below. This ANOVA model is reliable as supported by the residual plot in Figure 5.6 and it shows that the distribution of the probability plot for the five models is quite normal and there are no significant outliers. Further tests were conducted to detect the differences among the models using the 'Tukey pairwise comparison' technique as presented in Table 5.3. The results indicate that significant differences are revealed between SPPA & DF (p=0.003); MVSA & GAC (p=0.035); SPPA & GAC (p= 0.000); SPPA & SDM (p= 0.000) at 95% confidence level. Meanwhile, SPPA & MVSA also show a significant difference (p= 0.061) at the 90% confidence level.

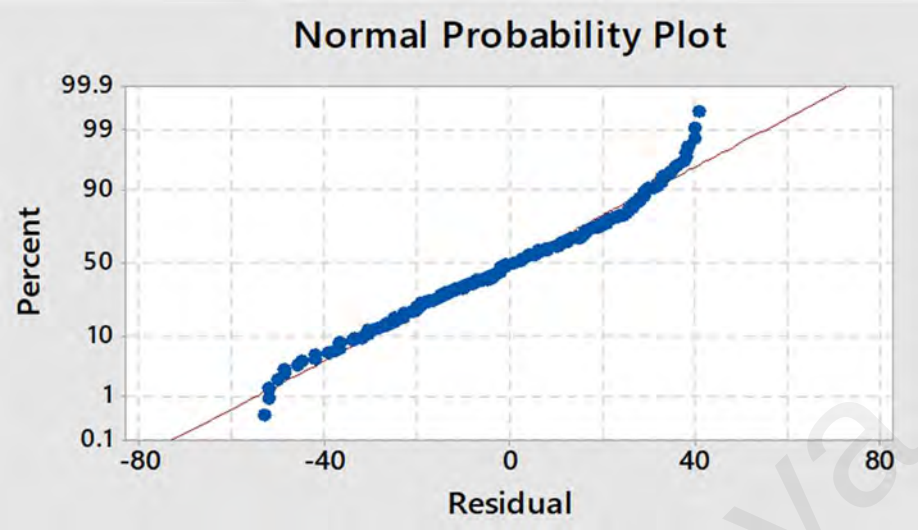

Figure 5.6: Residual Plots for Detection Rate

Table 5.3: Tukey Pairwise Comparison for Detection Rate

Difference of Levels	Difference of Means	SE of Difference	95% CI	T-Value	Adjusted P-Value
GAC - DF	-10.67	5.76	(-26.60, 5.27)	-1.85	0.349
MVSA - DF	6.03	5.76	(-9.90, 21.97)	1.05	0.833
SDM - DF	-5.70	5.76	(-21.63, 10.23)	-0.99	0.860
SPPA - DF	21.50	5.76	(5.57, 37.43)	3.73	**0.003**
MVSA - GAC	16.70	5.76	(0.77, 32.63)	2.90	**0.035**
SDM - GAC	4.97	5.76	(-10.97, 20.90)	0.86	0.910
SPPA - GAC	32.17	5.76	(16.23, 48.10)	5.58	**0.000**
SDM - MVSA	-11.73	5.76	(-27.67, 4.20)	-2.04	0.254
SPPA - MVSA	15.47	5.76	(-0.47, 31.40)	2.68	**0.061**
SPPA - SDM	27.20	5.76	(11.27, 43.13)	4.72	**0.000**

Note: - F-Test =9.33, P Value = 0.000

5.5.3 False Classification Ratio

The false classification has been performed in two ways - either classifying the true vehicle node as the false vehicle node or the false vehicle node as the true vehicle node. So, by

computing both, the false classification ratio can be calculated. For calculation we have used terms called TP and FP, where “TP” is True Positive, and “FP” is False Positive. The TP is also called true positive message rate of detection in some field.

Besides that, true positive refers to the number of genuine positive messages that are correctly recognized, for example the percentage of the genuine message which is properly recognized as having the issues. Another example is the case where a driver is actually attacked by DDoS (1) and the model classifies the case as DDoS Attack (1). Moreover, False Positive is also referred to as false alarm rate. The false positive itself denotes safety or non-safety messages incorrectly signalling seeing genuine issues such as security breaches or spam. For example, the percentage of genuine messages which are properly recognized as not having issues, such as where a driver NOT attacked by a DDoS and the model flags the case as a DDoS attack. Figure 5.7 demonstrates the false classification ratio as a function of true positive and false positive messages when the baseline models (MVSA & SPPA) are compared with the GAC, SDM and DF methods. Figure 5.7 shows the qualified examination of false classification ratio of the planned structure based on the values given below.

The SDM method has increased its false classification ratio for an average of 3% compared to the existing GAC method. Besides that, DF reduced its false classification ratio by 11% over SDM. The proposed first model MVSA has reduces its false classification ratio by 7% over the DF method. Also, the proposed second model, SPPA, has reduced its false classification ratio by 9% over the MVSA model.

From the analysis, it is clearly shown that the proposed second model, SPPA, has reduced its false classification ratio to 24%, as compared to the existing GAC methods. Finally, the MVSA has reduced its false classification ratio to 15%, as compared to the existing GAC method. Figure 5.7 clearly shows that the SPPA model consistently outperforms baseline approaches. This is due to the simplicity of the SPPA model in reducing the false classification ratio, and this approach was not merged with any other approach. Furthermore, in the work we have used conflict field, conflict data and attack signature sample to process each incoming packet and the SPPA model will detect the attack severity level whether its high impact node or low impact node. If its high impact nodes, in the future that particular node not able to communicate in the process. Moreover, the performance of all the approaches improves with time. A good model should reduce the false classification ratio (Mythili & Magendran, 2018). A misclassified packet will affect the performance of a vehicular network. Besides that, a good model should not classify a genuine packet as an attacked packet or an attacked packet as a genuine packet.

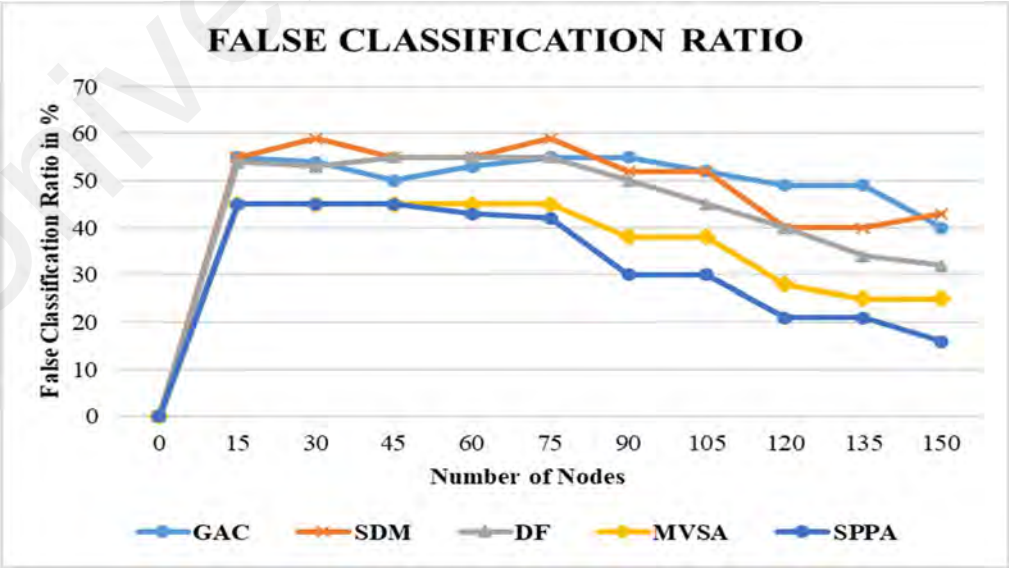

Figure 5.7: False Classification Results

5.5.3.1 Validation Results for False Classification Ratio

In the case of false classification ratio, results are presented in Table 5.4 below. This ANOVA model is reliable as supported by the residual plot in Figure 5.8 and it shows the distribution of the probability plot of the five models is quite normal and there are no significant outliers. Further tests were conducted to detect the differences among the models using the 'Tukey pairwise comparison' technique as presented in Table 5.10. The results indicate that significant differences are registered between GAC & DF (p=0.000); SPPA & DF (p= 0.000); MVSA & GAC (p= 0.000); SDM & GAC (p=0.019); SPPA & GAC (p= 0.000); SPPA & MVSA (p=0.000); SPPA & SDM (p= 0.000) at the 95% confidence level.

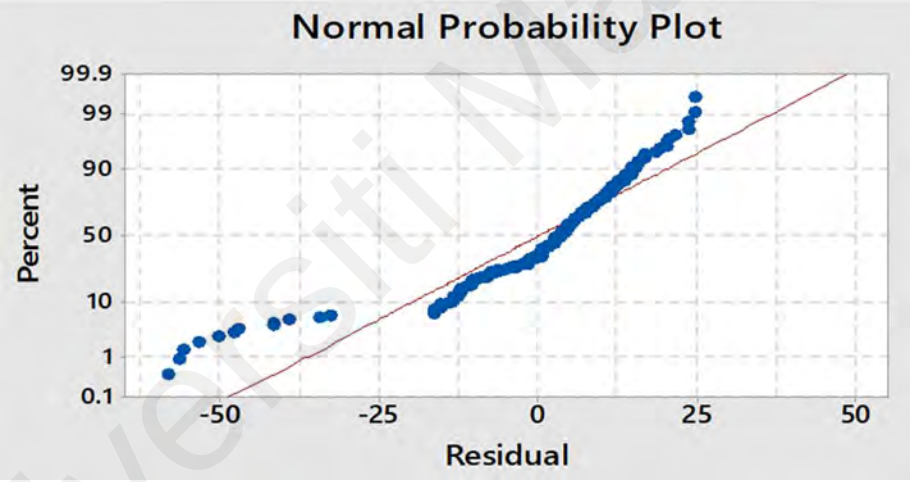

Figure 5.8: Residual Plots for False Classification Ratio

Table 5.4: Tukey Pairwise Comparison for False Classification Ratio

Difference of Levels	Difference of Means	SE of Difference	95% CI	T-Value	Adjusted P-Value
GAC - DF	17.77	4.20	(6.15, 29.38)	4.23	**0.000**
MVSA - DF	-3.37	4.20	(-14.98, 8.25)	-0.80	0.930
SDM - DF	4.70	4.20	(-6.92, 16.32)	1.12	0.796
SPPA - DF	-21.23	4.20	(-32.85, -9.62)	-5.05	**0.000**
MVSA - GAC	-21.13	4.20	(-32.75, -9.52)	-5.03	**0.000**

SDM - GAC	-13.07	4.20	(-24.68, -1.45)	-3.11	**0.019**
SPPA - GAC	-39.00	4.20	(-50.62, -27.38)	-9.28	**0.000**
SDM - MVSA	8.07	4.20	(-3.55, 19.68)	1.92	0.311
SPPA - MVSA	-17.87	4.20	(-29.48, -6.25)	-4.25	**0.000**
SPPA - SDM	-25.93	4.20	(-37.55, -14.32)	-6.17	**0.000**

Note: - F-Test =22.63, P Value = 0.000

5.5.4 Throughput

The throughput is measured with the usual rate of effective messages from vehicle source to vehicle destination. Moreover, the throughput evaluates the average amount of message per-second per vehicle, that will be delivered from vehicle source to vehicle destination. Throughput describes the amount of data packets established at a destination vehicle corresponding to the number of packets produced by the source vehicle for a specified period of time. Figure 5.9 demonstrates the throughput as a function of time when the baseline methods (MVSA & SPPA) are compared with the GAC, SDM and DF methods. It shows the qualified examination of throughput of the planned structure based on the values given in the graph.

The SDM method has improved its throughput, with 484 bytes over the existing GAC method in 200 Sec. Besides that, the DF method has improved its throughput by 850 bytes over the SDM method. The approach is tested over 200Sec. In addition, the proposed first model MVSA has improved its throughput by 1584 bytes over the DF method. Furthermore, the proposed second model SPPA has improved by an average of 1326 bytes over the MVSA method.

From the analysis, it is clearly shown that the proposed second model, SPPA, improved its throughput to 4245 bytes, as compared to the GAC method. Finally, the first proposed model, MVSA, improved its throughput to 2919 bytes, compared to the existing GAC method. Figure 5.9 clearly shows that the SPPA model consistently outperforms baseline approaches. This is due to the simplicity of the SPPA model in detecting DDoS attacks, and the approach was not merged with any other approach. Moreover, the performance of all the approaches improves with time. Furthermore, in the work we have used conflict field, conflict data and attack signature sample to process each incoming packet and the SPPA model will detect the attack severity level whether its high impact node or low impact node. If its high impact nodes, in the future that particular node not able to communicate in the process.

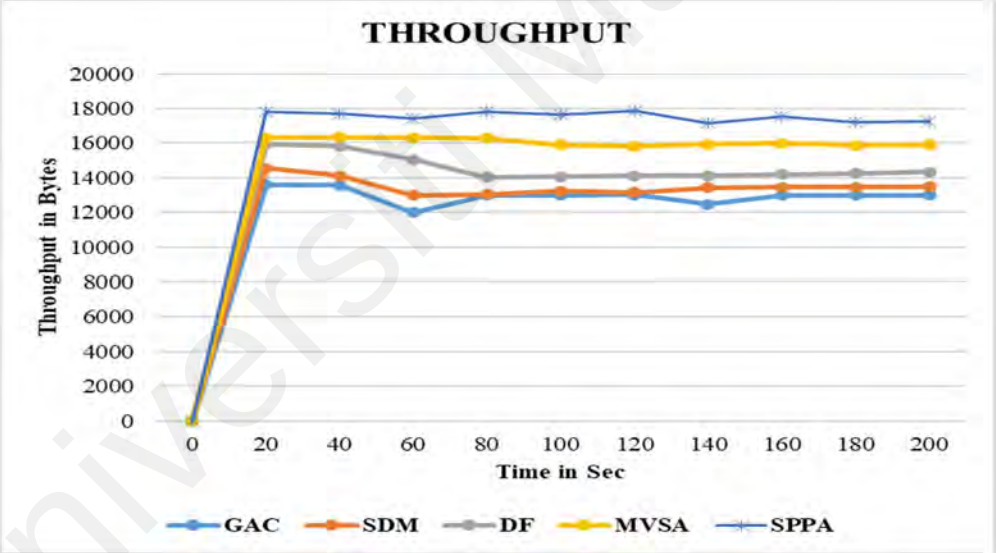

Figure 5.9 Throughput Results

5.5.4.1 Validation Results for Throughput

In the case of throughput, results are presented in Table 5.5 below. This ANOVA model is reliable as supported by the residual plot in Figure 5.10 and it shows that the distribution of the probability plot of the five models is quite normal and there are no significant outliers.

Further tests were conducted to detect the differences among the models using the 'Tukey pairwise comparison' technique as presented in Table 5.13. The results indicate that significant differences are revealed between MVSA & DF (p=0.000); MVSA & GAC (p=0.000); SDM & MVSA (p=0.000); SPPA & MVSA (p=0.000) at 95% confidence level.

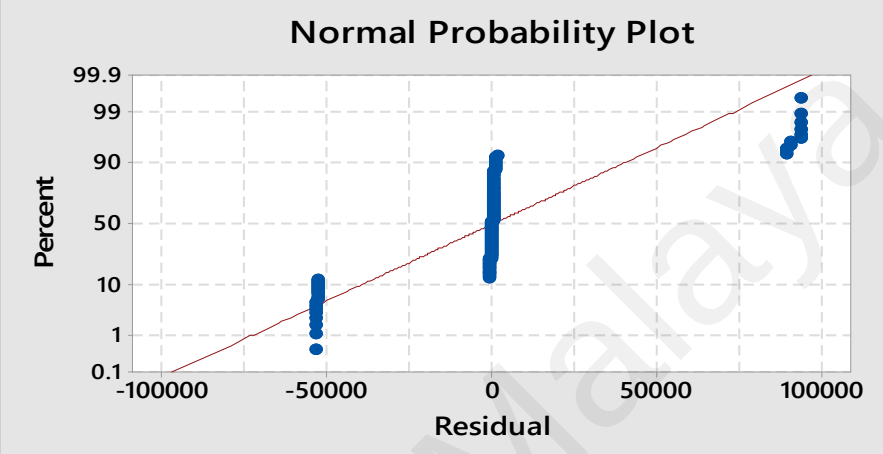

Figure 5.10: Residual Plots for Throughput

Table 5.5: Tukey Pairwise Comparison for Throughput

Difference of Levels	Difference of Means	SE of Difference	95% CI	T-Value	Adjusted P-Value
GAC – DF	-1515	8228	(-24264, 21234)	-0.18	1.000
MVSA – DF	55248	8228	(32499, 77997)	6.71	**0.000**
SDM – DF	-1186	8228	(-23935, 21563)	-0.14	1.000
SPPA – DF	3546	8228	(-19203, 26295)	0.43	0.993
MVSA – GAC	56763	8228	(34013, 79512)	6.90	**0.000**
SDM – GAC	328	8228	(-22421, 23078)	0.04	1.000
SPPA – GAC	5061	8228	(-17688, 27810)	0.62	0.973
SDM – MVSA	-56434	8228	(-79183, -33685)	-6.86	**0.000**
SPPA – MVSA	-51702	8228	(-74451, -28953)	-6.28	**0.000**
SPPA – SDM	4732	8228	(-18017, 27481)	0.58	0.979

Note: - F-Test =18.02, P Value = 0.000

5.5.5 End to End Delay

The time taken by the vehicle source node to convey the information effectively to the destination vehicle is called an end to end delay. It is the distinction between the time at which a packet was created by the vehicle source node and the time the packet reached the beneficiary or vehicle destination**.** In Figure 5.11, the end to end delay analysis of the proposed method compared with the existing method is demonstrated.

The different figures give the rate of sending packets specifically in seconds but sometimes a slight variation will be present. If the destination moves closer to the source node, then the delay will be decreased. Otherwise, the packet delay will be increased. The proposed models (MVSA & SPPA) are compared with the GAC, SDM and DF methods against the node variation from 0 to 150 nodes with a fixed speed. Moreover, it is clearly understood that the proposed SPPA model has reduced its end to end delay in the rate of sending packets.

The SDM method has an average reduction in end to end delay of 0.002 seconds over the existing GAC method. Moreover, the DF method has reduced its end to end delay with an average of 0.004 second over the SDM method. Next, the first proposed model MVSA has cut its end to end delay by an average of 0.003 seconds over the DF method. Finally, the proposed second model SPPA has cut its end to end delay by an average of 0.003 seconds over the MVSA model.

5.5.5.1 Validation Results for End to End Delay

In the case of end to end delay, results are presented in Table 5.6 below. This ANOVA model is reliable as supported by the residual plot in Figure 5.12 and it shows that the distribution

of the probability plot of the five models is quite normal and there are no significant outliers. Further tests were conducted to detect the differences among the models using the 'Tukey pairwise comparison' technique as presented in Table 5.6. The results indicate that significant differences are registered between GAC & DF (p=0.000); SPPA & DF (p= 0.000); MVSA & GAC (p= 0.000); SDM& GAC (p=0.000); SPPA & GAC (p= 0.000); SPPA & MVSA (p=0.000) and SPPA & SDM (p= 0.000) at the 95% confidence level.

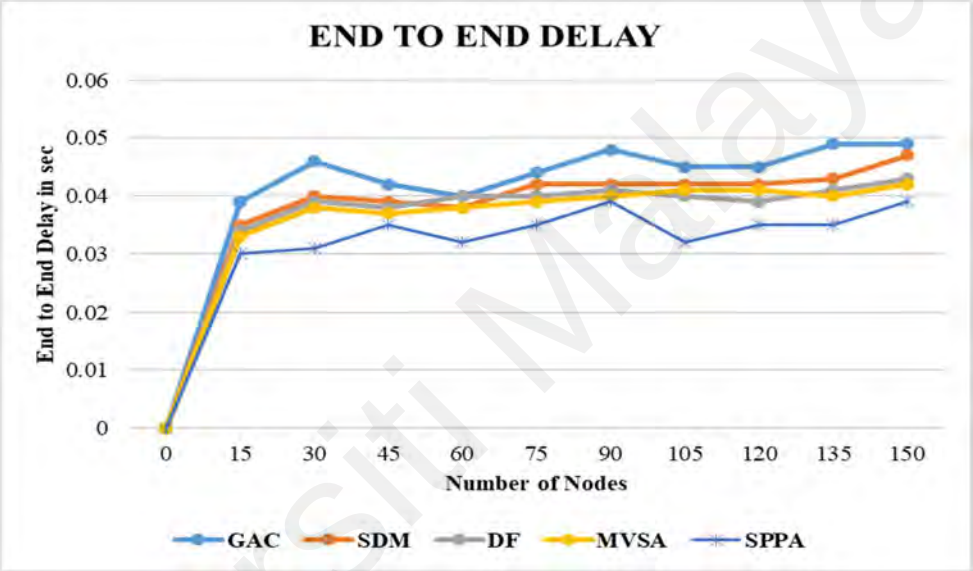

Figure 5.11: End to End Delay Results

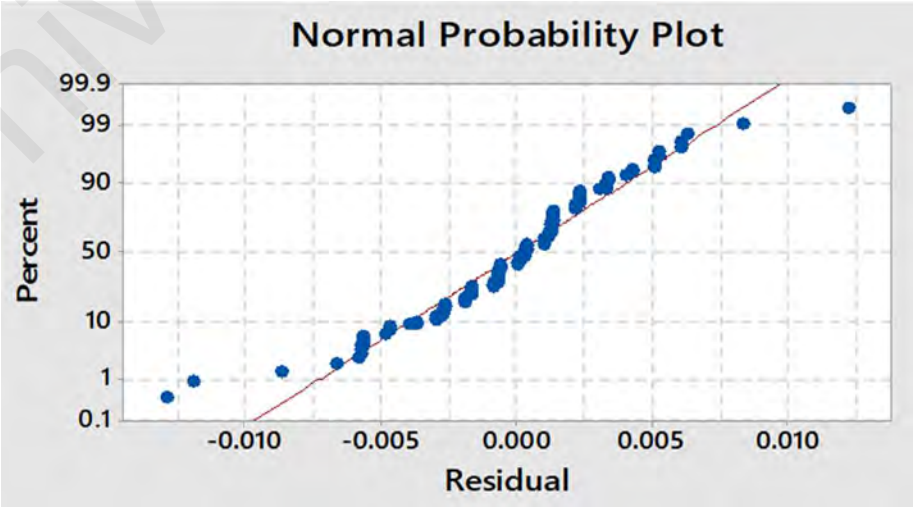

Figure 5.12: Residual Plots for End to End Delay

Table 5.6: Tukey Pairwise Comparison for End to End Delay

Difference of Levels	Difference of Means	SE of Difference	95% CI	T-Value	Adjusted P-Value
GAC - DF	0.005067	0.000874	(0.002650, 0.007483)	5.80	**0.000**
MVSA - DF	-0.000933	0.000874	(-0.003350, 0.001483)	-1.07	0.823
SDM - DF	0.001033	0.000874	(-0.001383, 0.003450)	1.18	0.762
SPPA - DF	-0.005700	0.000874	(-0.008117, -0.003283)	-6.52	**0.000**
MVSA - GAC	-0.006000	0.000874	(-0.008417, -0.003583)	-6.86	**0.000**
SDM - GAC	-0.004033	0.000874	(-0.006450, -0.001617)	-4.61	**0.000**
SPPA - GAC	-0.010767	0.000874	(-0.013183, -0.008350)	-12.32	**0.000**
SDM - MVSA	0.001967	0.000874	(-0.000450, 0.004383)	2.25	0.168
SPPA - MVSA	-0.004767	0.000874	(-0.007183, -0.002350)	-5.45	**0.000**
SPPA - SDM	-0.006733	0.000874	(-0.009150, -0.004317)	-7.70	**0.000**

Note: - F-Test =39.30, P Value = 0.000

5.5.6 Packet Delivery Ratio (PDR)

PDR is utilized to assess the nature of the vehicular to vehicular communication in VANET, due to an optimized analysis of incoming and outgoing of vehicle packets. Hence, it characterizes the proportion of packets received by a vehicle to packets produced by the vehicle source. It can be gained by utilizing awk content, which delivers the flow and the outcome. Figure 5.13 demonstrates the PDR as a function of messages received by the destination vehicle when the baseline models (MVSA & SPPA) are compared to the GAC, SDM and DF methods.

The SDM method had an average increase in PDR of 4.73% over the existing GAC method. Besides that, the SDM method recorded a 90% PDR value and DF method recorded a 92% PDR value. The both methods are increased its PDR with an average of 6.73% over the GAC method. Furthermore, the first proposed MVSA model has recorded 95% PDR value. It has

actually increased its PDR with an average of 3% over the DF and SDM methods. Finally, the proposed second model SPPA has improved by an average of 2% against the MVSA model. The proposed SPPA model outperforms other models in terms of PDR. The simulation results show that the PDR for both existing and proposed algorithms are calculated, and the proposed scheme provides a high PDR. The analysis clearly shows that the proposed SPPA model has improved its PDR to 11.73% over the existing GAC method, 7% compared to the SDM method and 5% compared to the DF method.

However, the proposed MVSA model has improved its PDR to 2% compared to the SPPA method. Figure 5.13 clearly shows that the SPPA model consistently outperforms baseline approaches. This is because the method and the measurement being used are based on the stability and performance of the VANET network. This is due to the simplicity of the SPPA model in detecting DDoS attacks, and the method was not merged with any other methods. Furthermore, in the work we have used conflict field, conflict data and attack signature sample to process each incoming packet and the SPPA model will checked each and every packet that come from the node. The CH in VANET will know entire information about the nodes. The SPPA is focused on the safety application traffic only. The rest of the existing models/methods are focused on the both traffics. SPPA model will detect the attack severity level whether its high impact node or low impact node. If its high impact nodes, in the future that particular node not able to communicate in the process.

5.5.6.1 Validation Results for Packet Delivery Ratio (PDR)

In the case of PDR, results are presented in Table 5.7 below. This ANOVA model is reliable as supported by the residual plot in Figure 5.14 and it shows that the distribution of the

probability plot of the five models is quite normal and there are no significant outliers. Further tests were conducted to detect the differences among the models using the 'Tukey pairwise comparison' technique as presented in Table 5.7. The results indicate that significant differences are recorded between MVSA & DF (p=0.000); SPPA & DF (p=0.000); MVSA & GAC (p= 0.000); SPPA & GAC (p= 0.000); SDM & MVSA (p=0.000); SPPA & SDM (p= 0.000) at 95% confidence level.

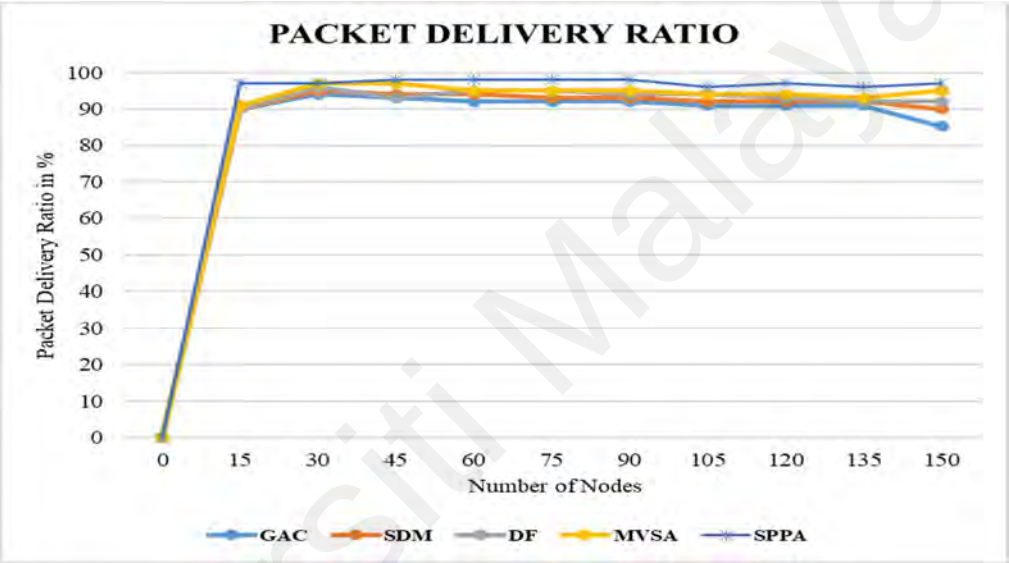

Figure 5.13 Packet Delivery Ratio Results

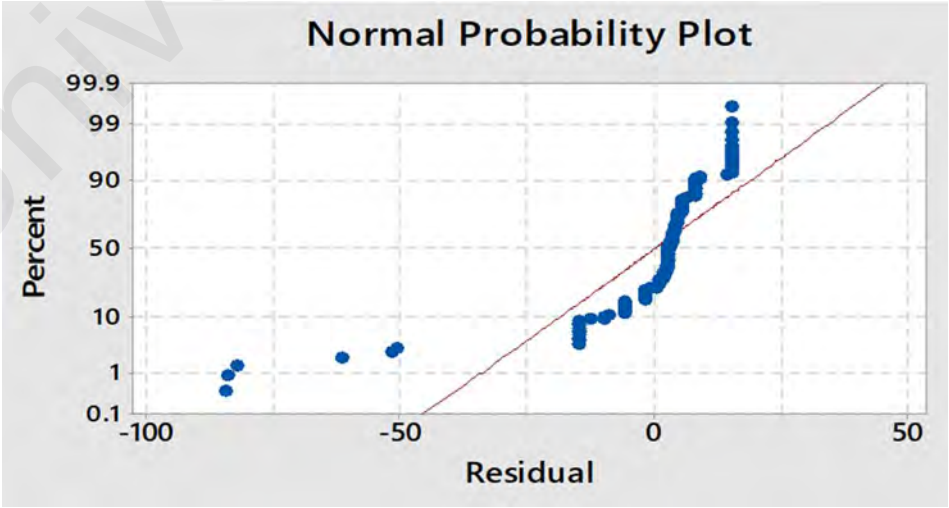

Figure 5.14: Residual Plots for Packet Delivery Ratio

Table 5.7: Tukey Pairwise Comparison for Packet Delivery Ratio

Difference of Levels	Difference of Means	SE of Difference	95% CI	T-Value	Adjusted P-Value
GAC - DF	-4.88	3.81	(-15.41, 5.66)	-1.28	0.704
MVSA - DF	17.70	3.81	(7.17, 28.23)	4.65	**0.000**
SDM - DF	-3.70	3.81	(-14.23, 6.83)	-0.97	0.868
SPPA - DF	19.70	3.81	(9.17, 30.23)	5.17	**0.000**
MVSA - GAC	22.58	3.81	(12.04, 33.11)	5.93	**0.000**
SDM - GAC	1.18	3.81	(-9.36, 11.71)	0.31	0.998
SPPA - GAC	24.58	3.81	(14.04, 35.11)	6.45	**0.000**
SDM - MVSA	-21.40	3.81	(-31.93, -10.87)	-5.62	**0.000**
SPPA - MVSA	2.00	3.81	(-8.53, 12.53)	0.52	0.985
SPPA - SDM	23.40	3.81	(12.87, 33.93)	6.14	**0.000**

Note: - F-Test =19.72, P Value = 0.000

5.5.7 Routing Overhead

The routing overhead is the number of routing packets mandatory for vehicle to vehicle communication in the VANET network. However, it is also essential for network communication. Normally the routing overhead will be calculated using an awk script by the progression on the trace file and will produce the outcomes. Figure 5.15 demonstrates the outcome of the Routing Overhead as a function of the frequent link breakages that lead to regular path failures for safety messages and non-safety messages. The baseline models (MVSA & SPPA) are compared with the existing methods GAC, SDM and DF. It shows a qualified examination of the Routing Overhead of the planned structure based on the values given in Figure 5.15. A good routing overhead should establish on-demand routes among source and destination nodes with less delay in connection setup and should not require a large amount of memory for communication.

The SDM method has decreased its Routing Overhead by 60 kbps packets by 150 nodes over the existing GAC method. The DF method decreased its Routing Overhead by 110 packets by 150 nodes compared to the SDM method. Furthermore, the first proposed MVSA method decreased its Routing Overhead by 104 packets by 150 nodes over the DF method. Finally, the proposed second model SPPA decreased its Routing Overhead by 309 packets by 150 vehicle nodes over the MVSA method.

The analysis clearly shows that the proposed third method, SPPA, has reduced its Routing Overhead to 583 kbps packets, as compared to the GAC method. Finally, the first proposed method MVSA has reduced its Routing Overhead to 274 packets, as compared to the existing GAC method. Figure 5.15 clearly shows that the SPPA method is consistently outperforming baseline approaches. This is due to the straightforwardness of the SPPA method in reducing Routing Overhead, and furthermore the method was not combined with any other approach. Moreover, the performance of Routing Overhead for all the methods are improved with time.

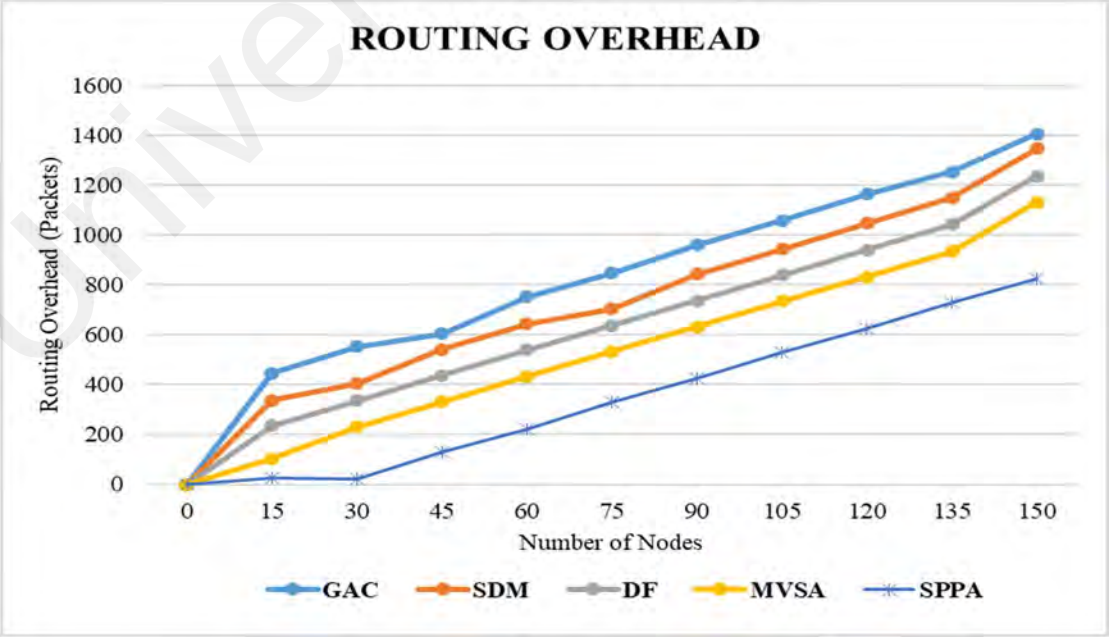

Figure 5.15: Routing Overhead Results

5.5.7.1 Validation Results for Routing Overhead

In the case of Routing Overhead, results are presented in Table 5.8 below. This ANOVA model is reliable as supported by the residual plot in Figure 5.16 and it shows that the distribution of the probability plot of the five models is quite normal and there are no significant outliers. Further tests were conducted to detect the differences among the models using the 'Tukey pairwise comparison' technique as presented in Table 5.22. The results indicate that there are significant differences between GAC & DF (p=0.025); SPPA & DF (p= 0.006); MVSA & GAC (p= 0.001); SPPA & GAC (p= 0.000); SPPA & SDM (p= 0.000) at the 95% confidence level. Meanwhile, SDM & MVSA and SPPA & MVSA also show a significant difference (p= 0.091; p=0.087) at the 90% confidence level.

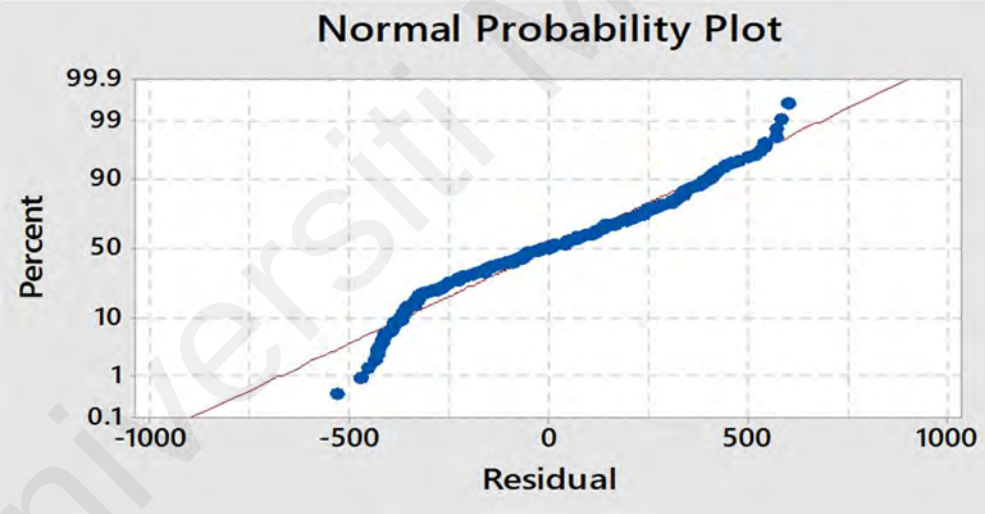

Figure 5.16: Residual Plots for Routing Overhead

Table 5.8: Tukey Pairwise Comparison for Routing Overhead

Difference of Levels	Difference of Means	SE of Difference	95% CI	T-Value	Adjusted P-Value
GAC - DF	232.7	77.3	(18.9, 446.5)	3.01	**0.025**
MVSA - DF	-72.0	77.3	(-285.8, 141.8)	-0.93	0.884
SDM - DF	131.0	77.3	(-82.8, 344.8)	1.69	0.441
SPPA - DF	-268.6	77.3	(-482.4, -54.8)	-3.47	**0.006**

MVSA - GAC	-304.7	77.3	(-518.5, -90.9)	-3.94	**0.001**
SDM - GAC	-101.7	77.3	(-315.5, 112.1)	-1.31	0.682
SPPA - GAC	-501.3	77.3	(-715.1, -287.5)	-6.48	**0.000**
SDM - MVSA	203.0	77.3	(-10.8, 416.8)	2.63	**0.071**
SPPA - MVSA	-196.6	77.3	(-410.4, 17.2)	-2.54	**0.087**
SPPA - SDM	-399.7	77.3	(-613.5, -185.9)	-5.17	**0.000**

Note: - F-Test =12.42, P Value = 0.000

5.6 Significance of Findings

The both proposed models (MVSA & SPPA) are better than the existing models/methods. In the MVSA model I have used 4 important features for example (Payload, Packet Frequency, Hop Count and TTL). The existing models/methods are used position & mobility of vehicle, speed of the vehicle, direction of the vehicle, time stamp, threshold, packet flow, packet ID, payload, and location. The features combination that I have used no one else have used to simulate the DDoS attack detection in VANET. At the same time, I have used packet classification stage to classify and identify the important packet before its block or drops. Moreover, the MVSA method will follow the marking stage. The packet marking is used to trace back to the source node and all the intermediate node. Request the info from the origin node that located in RSU. If there is any modification that particular node will terminate from the process. Therefore, the method is able to produce better results based on the 7-performance metrics. The SPPA model is used for time efficiency to detect the DDoS attack in in 0.08 seconds. This is one of the fastest detection time based on the simulation. This model performs in the efficient way because we have used clustering based attacked detection. At the same time, we have used CCA mechanism and attack severity level. This both are the main contribution of the SPPA model. The Efficiency was proven based on the false classification performance metric. A good model should reduce the false classification

ratio to show the efficiency of the model (Mythili & Magendran, 2018). I have tested with 150 nodes in the Ns2 simulation for SPPA model and 50 nodes for MVSA. Based on the 7-performance metrics. It showed that the model is improved from the existing models/methods. Most of the existing models/methods is used throughput metric, PDR metrics, Packet Loss metric, communication loss metrics and Attack detection time. In this work I have used 7 performance metrics and its divided into 2; first DDoS metrics and second is network metrics. Each model is improved due to the efficiency of the method and features that we used to detect the DDoS attacks. Moreover, the classification, CCA and attack severity level steps that used is more unique to show the differences among other models/methods.

5.7 Conclusion

The primary purpose of this research is to determine the relative importance of DDoS attack detection. It is achieved by necessity to reach some significant goals based on the proposed algorithms such as Multi Variant Stream Analysis and Stream Position Performance Analysis Model algorithms. To provide for the possibility that DDoS attack detection could be perceived and measured as a feasible component, it is important to develop a potential model. Once these fundamental steps are achieved, this research is able to go forward. This chapter presented the details of outcomes generated by the different techniques and the methods evaluated for many parameters, and the methods provided effective results. Finally, the author has validated the proposed model.

CHAPTER 6: CONCLUSIONS AND FUTURE DIRECTIONS

This chapter presents concluding remarks to the work presented in this thesis. Therefore, it starts by giving an overview of the problem statement in Section 6.1. Thereafter, a review of achieved objectives is presented in Section 6.2. The chapter then summarizes the contributions and gives some future direction in Section 6.3 and Section 6.4 respectively.

6.1 Overview

The motivation for Intelligent Transportation System (ITS) is to develop technologies that can be used by people in transportation systems to reduce accidents and provide some comfort through infotainment. On the road, ITS applications are envisaged to be transmitted through vehicular communication using Dedicated Short-Range Communication (DSRC) channels. At that particular time, attacks can happen. Moreover, the DDoS attack detection system has an extensive effect on the performance of the vehicular environment, particularly the vehicle to vehicle communication and RSU services. Aware of the trouble, researchers have come up with many strategies. Still, they aim to attain the required performance in DDoS attack detection and have an incentive to improve the performance of attack detection in vehicle to vehicle communication. The researcher has proposed 2 different frameworks, namely MVSA and SPPA. The MVSA is used for small scale applications and for large scale contexts, the SPPA method is used.

6.2 Reappraisal of Achieved Objectives

This thesis presented an efficient DDoS attack detection framework for vehicular communications. To achieve this aim, 4 specific objectives were outlined in Chapter 1. The first objective was to explore characteristics of DDoS Attacks in VANET. The second

objective was to design and develop frameworks for detecting a DDoS attack in the vehicular environment. The third objective was to evaluate the framework using a Network Simulator and to benchmark the proposed framework against existing models. The fourth objective is to validate the proposed framework using statistical tools. The following details how each of these objectives have been achieved in this thesis.

- **To explore characteristics of DDoS Attacks in VANET** – the literature has been reviewed, including background studies of DDoS attack detection methods from VANETs, MANETs, Cloud, Network and Cluster. The background studies are presented in Chapter 2. Additionally, this thesis has discussed attacks on vehicular networks, components of VANETs and discussed safety applications and non-safety applications. Moreover, the problem analysis was discussed in Chapter 3. In the chapter some comparison on performance metrics was carried out with 10 methods that are more relevant and there has been a discussion of journal article statistics for DoS and DDoS attacks in VANET from 2009 – 2018.

- **To design and develop frameworks for detecting a DDoS attack in the vehicular environment** – Chapter 4 discussed the framework consisting of Multi Variant Stream Analysis (MVSA) and Stream Position Performance Analysis (SPPA). The first model is an efficient Multi Variant Stream Analysis (MVSA) method to detect DDoS attacks. At first the model will identify the size of the traffic and send it to pre-processing stage. Then the vehicle reads the network trace and computes an average measure of payload, time-to-live, and the frequency for each stream class at different time windows. Four features are measured and computed in the methods to generate the rule set. The rule set is generated, and the features are extracted from the packet

received from the user. Nevertheless, the method computes the Multi Variant Stream Weight. Moreover, the process will continue with the marking process. By using the computed stream weight and outcomes from the marking process, the method classifies packets into either malicious or genuine. The method was shown to be efficient in detecting DDoS attacks in vehicular communication and subsequently reduced the impact on the VANET environment. The second model is called Stream Position Performance Analysis (SPPA). This method is used for large scale vehicular communication. Additionally, in the proposed SPPA model, the detection of a DDoS attack is based on the computed value of the Conflict Field, Conflict Data and Attack Signature Sample (CCA). The behaviour of each and every node is evaluated, and the legitimate weight of the node is calculated. Using this legitimate weight, the attack detection is performed by analyzing whether the node is an intruder or normal node. Finally, it will classify the categories as high impact or low impact node. The proposed method's evaluation result reduces the end to end delay and overhead occurred in the complex vehicular network and improves the detection time and routine of the network.

- **To evaluate the framework using a Network Simulator and to benchmark the proposed framework against existing models.** In this work, evaluation of the proposed framework was only possible through simulation. Therefore, Chapter 4 is dedicated to discussing simulation tools used in this work. Particularly, SUMO tools and the Ns2 were discussed in Chapter 5. Evaluation of the framework based on the results from the simulation is presented in Chapter 5. The proposed framework consists of two models and the models are compared to three existing models/methods. The models are A Group Adaptive Controller-based Method (GAC)

(Vipin & Chhillar, 2018), Sentinel: Defense Mechanism Against DDoS Flooding Attack in Software Defined Vehicular Network (SDM) (Biasi et al., 2018) and A Novel Security Approach for Data Flow and Data Pattern Analysis to Mitigate DDoS attacks in VANETs (DF) (Kaur & Mahajan, 2015).

- **To validate the proposed framework using statistical tools**. This objective aimed to validate the results from MVSA, SPPA, GAC, SDM and DF. To validate the results from the simulation, Minitab version 18 was used, because it will give robust results. At the same time, this research has showed Tukey Anova comparison tables and identified the significant results among the 5 models. Chapter 5 discusses the types of statistical tools and their importance.

6.3 Findings and Contribution

The study is valuable for VANET users as it offers a new set of concepts, specifically in the area of security. VANET has provided the wireless communication network in order to manage road traffic. By implementing the VANET in the ITS, every vehicle can communicate with each other through the RSU and OBU. The researcher has proposed a framework to detect DDoS attacks in VANET environments. The first framework is Multi Variant Stream Analysis (MVSA), and the second framework is Stream Position Performance Analysis (SPPA). Attack detection is performed by analyzing whether the node is an intruder or a normal node. The simulation outcomes have been concluded to validate the proposed detection measures. The proposed method after evaluation reduces the Attack Detection Time, Packet Drop Ratio and overheads that occur in the complex VANET network.

6.4 Future Directions

The vehicular networks are a novel class of wireless networks. Vehicular networks are spontaneously formed between moving vehicles equipped with wireless interfaces that could be of homogeneous or heterogeneous technologies. These networks, also known as VANETs, is considered as one of the ad hoc network real-life applications enabling communication among nearby vehicles as well as between vehicles and nearby fixed equipment, usually described as roadside equipment.

Vehicles can be either private, belonging to individuals or private companies, or public transportation means (e.g., buses and public service vehicles such as police cars). Fixed equipment can belong to the government or private network operators or service providers. VANET is completely a mobile network whose nodes consists of vehicles equipped with wireless routers and a human machine interface that acts as a heads-up display for warnings and as a display monitor for business/infotainment services.

There are still several issues regarding the attacks on VANET that permit further research as the existing system may connect multiple paths in networks. The DDoS attacks are a growing hazard through the Internet, hard contact with materials and services. Our future research is on Markov Chain-Based Ant Colony approach for mitigating DDoS attacks using integrated vehicle mode analysis in VANET. The underlying assumption is that a Ant colony analysis of vehicles specifies reliability and unreliability of messages they drive. With Ant colony, all evident information on a vehicle is submitted to provide past, current and even prospect activities and its transmission activities. We need to perform number of classifications from the data we receive from ant colony analysis and its permits a significant analysis. We can name it as hybrid model or enhancement model.

REFERENCES

Agrawal, A., Garg, A., Chaudhiri, N., Gupta, S., Pandey, D., & Roy, T. (2013). Security on vehicular ad hoc networks (VANET): A review paper. *International Journal of Emerging Technology and Advanced Engineering*, *3*(1), 231-235.

Ahmad, A. M., Idriss, H., El Mouallem, A., & El Bazzal, Z. (2018). Chain-based data dissemination in vehicular ad-hoc networks (VANETs). In *2018 Sixth International Conference on Digital Information, Networking, and Wireless Communications (DINWC)* (pp. 75-80). IEEE.

Ahmad, I., Ashraf, U., & Ghafoor, A. (2016). A comparative QoS survey of mobile ad hoc network routing protocols. *Journal of the Chinese Institute of Engineers*, *39*(5), 585-592.

Alexiou, N., Laganà, M., Gisdakis, S., Khodaei, M., & Papadimitratos, P. (2013). Vespa: Vehicular security and privacy-preserving architecture. In *Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy* (pp. 19-24). ACM.

Alheeti, K. M. A., Gruebler, A., & McDonald-Maier, K. (2017). Using discriminant analysis to detect intrusions in external communication for self-driving vehicles. *Digital Communications and Networks*, *3*(3), 180-187.

Al-Hourani, A., Chandrasekharan, S., Baldini, G., & Kandeepan, S. (2014). Propagation measurements in 5.8 GHz and pathloss study for CEN-DSRC. In *2014 International Conference on Connected Vehicles and Expo (ICCVE)* (pp. 1086-1091). IEEE.

Al-Qutayri, M., Yeun, C., & Al-Hawi, F. (2010). Security and privacy of intelligent VANETs. In *Computational Intelligence and Modern Heuristics*. IntechOpen.

Alwakeel, S., & Prasetijo, A. (2014). A virtual P-Persistent bandwidth partitioning manager for VANET's broadcast channel. In *2014 International Conference on Multimedia Computing and Systems (ICMCS)* (pp. 1212-1215). IEEE.

Amine, D., Nasr-Eddine, B., & Abdelhamid, L. (2015). A distributed and safe weighted clustering algorithm for mobile wireless sensor networks. *Procedia Computer Science*, *52*, 641-646.

Andrysiak, T., Saganowski, Ł., & Choraś, M. (2013). DDoS attacks detection by means of greedy algorithms. In *Image Processing and Communications Challenges 4* (pp. 303-310). Springer, Berlin, Heidelberg.

Ayonija Pathre, C., & Jain, A. (2013) Identification of malicious vehicle in VANET Environment from DDOS attack. *Journal of Global Research in Computer Science 4*. 30-34.

Azees, M., Vijayakumar, P., & Deborah, L. J. (2016). Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intelligent Transport Systems*, *10*(6), 379-388.

Azogu, I. K., Ferreira, M. T., Larcom, J. A., & Liu, H. (2013, December). A new anti-jamming strategy for VANET metrics-directed security defense. In *2013 IEEE Globecom Workshops (GC Wkshps)* (pp. 1344-1349). IEEE.

Balan, E. V., Priyan, M. K., Gokulnath, C., & Devi, G. U. (2015). Fuzzy based intrusion detection systems in MANET. *Procedia Computer Science*, *50*, 109-114.

Bansal, E. P., & Pawar, E. L. (2015). Reducing impact of flooding in VANET due to distributed Denial of service attacks. *IJESC*.

Bansal, P., Sharma, S., & Prakash, A. (2015). A Novel approach for Detection of Distributed Denial of Service attack in VANET. *International Journal of Computer Applications*, *120*(5).

Bariah, L., Shehada, D., Salahat, E., & Yeun, C. Y. (2015). Recent advances in VANET security: a survey. Presented in *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)* (pp. 1-7). IEEE.

Barskar, R., & Chawla, M. (2015). Vehicular Ad Hoc Networks and its Applications in Diversified Fields. *International Journal of Computer Applications,123*, 7-11.

Bhuyan, M. H., Kashyap, H. J., Bhattacharyya, D. K., & Kalita, J. K. (2013). Detecting distributed denial of service attacks: methods, tools and future directions. *The Computer Journal*, *57*(4), 537-556.

Bhoi, S. K., Khilar, P. M., Singh, M., Sahoo, R. R., & Swain, R. R. (2018). A routing protocol for urban vehicular ad hoc networks to support non-safety applications. *Digital Communications and Networks, 4*(3), 189-199.

Biswas, S., Mišić, J., & Mišić, V. (2012). DDoS attack on WAVE-enabled VANET through synchronization. Presented in 2012 IEEE Global Communications Conference (GLOBECOM) (pp. 1079-1084). IEEE.
Kakoty, B. S., Hazarika, S. M., & Sarma, N. (2013). NAODV-Distributed Packet Dropping Attack Detection in MANETs. *International Journal of Computer Applications*, *83*(11)

Burmester, M., Magkos, E., & Chrissikopoulos, V. (2008). Strengthening privacy protection in vanets. Presented in *2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications* (pp. 508-513). IEEE.

Cepheli, Ö., Büyükçorak, S., & Karabulut Kurt, G. (2016). Hybrid intrusion detection system for ddos attacks. Journal of Electrical and Computer Engineering, 2016.

Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network Intrusion Detection for IoT Security based on Learning Techniques. *IEEE Communications Surveys & Tutorials*.

Chadha, D., & R. (2015). Vehicular Ad hoc Network (VANETs): A review. *International Journal of Innovative Research in Computing and Communication Engineering,3*(3), 2339-2346.

Chaubey, N. K. (2016). Security analysis of vehicular ad hoc networks (VANETs): a comprehensive study. *International Journal of Security and Its Applications*, *10*(5), 261-274.

Chen, J., Tang, X., Cheng, J., Wang, F., & Xu, R. (2019). DDoS attack detection method based on network abnormal behavior in big data environment. *arXiv preprint arXiv:1903.11844*.

Chen, R., Ma, D., & Regan, A. (2009). TARI: Meeting delay requirements in VANETs with efficient authentication and revocation. Presented in *2nd International Conference on Wireless Access in Vehicular Environments (WAVE)*.

Chen, W., Guha, R. K., Kwon, T. J., Lee, J., & Hsu, Y. Y. (2011). A survey and challenges in routing and data dissemination in vehicular ad hoc networks. *Wireless Communications and Mobile Computing*, *11*(7), 787-795.

Chikhaoui, O., Chehida, A. B., Abassi, R., & El Fatmi, S. G. (2017). A ticket-based authentication scheme for VANETs preserving privacy. Presented in *International Conference on Ad-Hoc Networks and Wireless* (pp. 77-91). Springer, Cham.

Chikhaoui, O., Douss, A. B. C., Abassi, R., & El Fatmi, S. G. (2018). Towards the Formal Validation of a Ticket-Based Authentication Scheme for VANETs. Presented in *32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)* (pp. 496-501). IEEE.

Da Cunha, F. D., Boukerche, A., Villas, L., Viana, A. C., & Loureiro, A. A. (2014). *Data communication in VANETs: a survey, challenges and applications* (Doctoral dissertation, INRIA Saclay; INRIA).

Dahane, A., Loukil, A., Kechar, B., & Berrached, N. E. (2015). Energy efficient and safe weighted clustering algorithm for mobile wireless sensor networks. Mobile information systems, *(2015)*

de Biasi, G., Vieira, L.F. and Loureiro, A.A. (2018). Sentinel: Defense mechanism against DDoS flooding attack in Software Defined Vehicular Network. Presented in 2018 *IEEE International Conference on Communications* (ICC) (pp. 1-6). IEEE.

De La Torre, G., Rad, P., & Choo, K. K. R. (2018). Driverless vehicle security: Challenges and future research opportunities. *Future Generation Computer Systems*.

Deny, J., & Sivasankari, N. (2011) Implementation of high security in MANET using combined IDS and Fingerprint Authentication with Data Fusion. *(IJCSIT) International Journal of Computer Science and Information Technologies, 2*(5) *, 2213-2215.*

Deshpande, S. G. (2013). Classification of Security attack in Vehicular Adhoc network: A survey. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, *2*(2), 371-377.

Dhaka, A., Nandal, A., & Dhaka, R. S. (2015). Gray and black hole attack identification using control packets in MANETs. *Procedia Computer Science*, *54*, 83-91.

Diaz, A., & Sanchez, P. (2016). Simulation of attacks for security in wireless sensor network. Sensors, 16(11), 1932.

Doss, S., Nayyar, A., Suseendran, G., Tanwar, S., Khanna, A., & Thong, P. H. (2018). APD-JFAD: accurate prevention and detection of jelly fish attack in MANET. *IEEE Access*, *6*, 56954-56965.

Eichler, S. (2007). Performance evaluation of the IEEE 802.11 p WAVE communication standard. Presented In *2007 IEEE 66th Vehicular Technology Conference* (pp. 2199-2203). IEEE.

Elhoseny, M., Elminir, H., Riad, A., & Yuan, X. (2016). A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption. *Journal of King Saud University-Computer and Information Sciences*, *28*(3), 262-275.

Elsadig, M. A., & Fadlalla, Y. A. (2016). VANETs security issues and challenges: a survey. *Indian Journal of Science and Technology*, *9*(28), 1-8.

Engoulou, R. G., Bellaïche, M., Pierre, S., & Quintero, A. (2014). VANET security surveys. *Computer Communications*, *44*, 1-13.

Eze, E. C., Zhang, S. J., Liu, E. J., & Eze, J. C. (2016). Advances in vehicular ad-hoc networks (VANETs): Challenges and road-map for future development. *International Journal of Automation and Computing*, *13*(1), 1-18.

Eze, E. C., Zhang, S., & Liu, E. (2014, September). Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward. In *2014 20th International Conference on Automation and Computing* (pp. 176-181). IEEE.

Faezipour, M., Nourani, M., Saeed, A., & Addepalli, S. (2012). Progress and challenges in intelligent vehicle area networks. *Communications of the ACM*, *55*(2), 90-100.

Fragkiadakis, A. G., Siris, V. A., Petroulakis, N. E., & Traganitis, A. P. (2015). Anomaly-based intrusion detection of jamming attacks, local versus collaborative detection. *Wireless Communications and Mobile Computing*, *15*(2), 276-294.

Fung, C. J., & Zhu, Q. (2016). FACID: A trust-based collaborative decision framework for intrusion detection networks. *Ad Hoc Networks*, *53*, 17-31.

Fotohi, R., Ebazadeh, Y., & Geshlag, M. S. (2016). A new approach for improvement security against DoS attacks in vehicular ad-hoc network. *International Journal of Advanced Computer Science and Applications*, *7*(7), 10-16.

Gadkari, M. Y., & Sambre, N. B. (2012). VANET: routing protocols, security issues and simulation tools. *IOSR Journal of Computer Engineering*, *3*(3), 28-38.

Ghaleb, F. A., Razzaque, M. A., & Isnin, I. F. (2013). Security and privacy enhancement in vanets using mobility pattern. In *2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN)* (pp. 184-189). IEEE.

Ghorsad, S. A., Karde, P. P., Thakare, V. M., & Dharaskar, R. V. (2014). DoS attack detection in vehicular ad-hoc network using malicious node detection algorithm. *International Journal of Electronics, Communication and Soft Computing Science & Engineering (IJECSCSE)*, *3*, 36.

Gillani, S., Shahzad, F., Qayyum, A., & Mehmood, R. (2013, May). A survey on security in vehicular ad hoc networks. In *International Workshop on Communication Technologies for Vehicles* (pp. 59-74). Springer, Berlin, Heidelberg.

Grover, J., Laxmi, V., & Gaur, M. S. (2013). Attack models and infrastructure supported detection mechanisms for position forging attacks in vehicular ad hoc networks. *CSI transactions on ICT*, *1*(3), 261-279.

Gupta, B. B., Joshi, R. C., & Misra, M. (2012). ANN Based Scheme to Predict Number of Zombies in a DDoS Attack. *IJ Network Security*, *14*(2), 61-70.

Hafeez, K. A., Zhao, L., Liao, Z., & Ma, B. N. W. (2010). Impact of mobility on vanets' safety applications. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010* (pp. 1-5). IEEE.

Hamida, E., Noura, H., & Znaidi, W. (2015). Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures. *Electronics*, *4*(3), 380-423.

Harpreet K., & Supreet, K. (2015). Security mechanism for Collision Avoidance and Attack Prevention Formants. *International Journal of Computer Trends and Technology (IJCTT)*. *23*(2), 73-75.

Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2017). VANET security challenges and solutions: A survey. *Vehicular Communications*, *7*, 7-20.

He, J., Tang, Z., O'Farrell, T., & Chen, T. M. (2011). Performance analysis of DSRC priority mechanism for road safety applications in vehicular networks. *Wireless Communications and Mobile Computing*, *11*(7), 980-990.

Ho, K. Y., Kang, P. C., Hsu, C. H., & Lin, C. H. (2010). Implementation of WAVE/DSRC devices for vehicular communications. In *2010 International Symposium on Computer, Communication, Control and Automation (3CA)*(pp. 522-525). IEEE.

Hussain, R., & Oh, H. (2014). Cooperation-Aware VANET Clouds: Providing Secure Cloud Services to Vehicular Ad Hoc Networks. *JIPS*, *10*(1), 103-118.

Hussein, A., Elhajj, I. H., Chehab, A., & Kayssi, A. (2017). SDN VANETs in 5G: An architecture for resilient security services. In *2017 Fourth International Conference on Software Defined Systems (SDS)* (pp. 67-74). IEEE.

Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative AwarenessBasic Service. European Telecommunications Standards Institute ETSI TS 302 637-2 v1.3.0; 2013.

Ismail, M. N., Aborujilah, A., Musa, S., & Shahzad, A. (2013). Detecting flooding-based DoS attack in cloud computing environment using covariance matrix approach. In *Proceedings of the 7th international conference on ubiquitous information management and communication* (p. 36). ACM.

Iyengar, N. C. S., & Ganapathy, G. (2015). Trilateral trust-based defense mechanism against DDoS attacks in cloud computing environment. *Cybernetics and Information Technologies*, *15*(2), 119-140.

Jafari, A., Al-Khayatt, S., & Dogman, A. (2012). Performance evaluation of IEEE 802.11 p for vehicular communication networks. In *2012 8th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP)* (pp. 1-5). IEEE.

Jeffane, K., & Ibrahimi, K. (2016). Detection and identification of attacks in Vehicular Ad-Hoc NETwork. In 2016 *International Conference on Wireless Networks and Mobile Communications (WINCOM)* (pp. 58-62). IEEE.

Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In Mobile computing (pp. 153-181). Springer, Boston, MA.

Jiang, D., & Delgrossi, L. (2008, May). Towards an international standard for wireless access in vehicular environments. In *VTC Spring 2008-IEEE Vehicular Technology Conference* (pp. 2036-2040). IEEE.

Jingle, I. D. J., & Rajsingh, E. B. (2014). ColShield: An effective and collaborative protection shield for the detection and prevention of collaborative flooding of DDoS attacks in wireless mesh networks. *Human-centric Computing and Information Sciences*, *4*(1), 8.

Karimazad, R., & Faraahi, A. (2011). An anomaly-based method for DDoS attacks detection using RBF neural networks. In *Proceedings of the International Conference on Network and Electronics Engineering* (pp. 44-48).

Kaur, G., & Sandhu, R. K. (2016). Effects of DDoS Attacks on Inter-Vehicle Communication - A survey. *International Journal of Computer Trends and Technology, 34(2),* 75-79.

Kaur, M., & Mahajan, M. (2015). A novel security approach for data flow and data pattern analysis to mitigate ddos attacks in vanets. *International Journal of Hybrid Information Technology*, *8*(8), 113-122.

Kaur, T., Toor, A. S., & Saluja, K. K. (2014). Defending MANETs against flooding attacks for military applications under group mobility. In *2014 Recent Advances in Engineering and Computational Sciences (RAECS)* (pp. 1-6). IEEE.

Kaushik, S. S. (2013). Review of different approaches for privacy scheme in VANETs. *International Journal of Advances in Engineering & Technology*, *5*(2), 356.

Kenney, J. B. (2011). Dedicated short-range communications (DSRC) standards in the United States. *Proceedings of the IEEE*, *99*(7), 1162-1182.

Kim, Y., Kim, I., & Shim, C. Y. (2014). A taxonomy for DOS attacks in VANET. In *2014 14th International Symposium on Communications and Information Technologies (ISCIT)* (pp. 26-27). IEEE.

Kukshya, V., & Krishnan, H. (2006). Experimental measurements and modeling for vehicle-to-vehicle Dedicated Short Range Communication (DSRC) wireless channels. In *IEEE Vehicular Technology Conference* (pp. 1-5). IEEE.

Kumar, A., & Sinha, M. (2014). Overview on vehicular ad hoc network and its security issues. In *2014 International conference on computing for sustainable global development (INDIACom)* (pp. 792-797). IEEE.

Kumar, V., Mishra, S., & Chand, N. (2013). Applications of VANETs: present & future. *Communications and network*, *5*(01), 12.

La Vinh, H., & Cavalli, A. R. (2014). Security attacks and solutions in vehicular ad hoc networks: a survey. *International Journal on AdHoc Networking Systems (IJANS), 4(2), 1-20.*

Li, J., Lu, H., & Guizani, M. (2015). ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. *IEEE Transactions on Parallel and Distributed Systems*, *26*(4), 938-948.

Li, L., & Lee, G. (2015), DDoS attack detection and wavelets. Telecommunication Systems. *28*(3-4), 435-451.

Li, Y. J. (2010). An overview of the DSRC/WAVE technology. In *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*(pp. 544-558). Springer, Berlin, Heidelberg.

Liang, W., Li, Z., Zhang, H., Sun, Y., & Bie, R. (2014). Vehicular ad hoc networks: Architectures, research issues, challenges and trend. In *International Conference on Wireless Algorithms, Systems, and Applications* (pp. 102-113). Springer, Cham.

Liang, W., Li, Z., Zhang, H., Wang, S., & Bie, R. (2015). Vehicular ad hoc networks: Architectures, research issues, methodologies, challenges, and trends. *International Journal of Distributed Sensor Networks*, *11*(8), 745303.

Liu, Q., Wu, Q., & Yong, L. (2013). A hierarchical security architecture of VANET.

Lott, M., Meincke, M., & Halfmann, R. (2004). A new approach to exploit multiple frequencies in DSRC. In *2004 IEEE 59th Vehicular Technology Conference. VTC 2004-Spring (IEEE Cat. No. 04CH37514)* (Vol. 3, pp. 1539-1543). IEEE.

Ma, X., Chen, X., & Refai, H. H. (2009). Performance and reliability of DSRC vehicular safety communication: A formal analysis. *EURASIP Journal on Wireless Communications and Networking*, (1), 969164.

Mansfield, D. S. (2015). The growth and evolution of DDoS. *Network Security*, (10), 13-20.

Manvi, S. S., & Tangade, S. (2017). A survey on authentication schemes in VANETs for secured communication. *Vehicular Communications*, *9*, 19-30.

Mehta, K., Malik, L. G., & Bajaj, P. (2013). VANET: Challenges, issues and solutions. In *2013 6th International Conference on Emerging Trends in Engineering and Technology* (pp. 78-79). IEEE.

Mejri, M. N., & Ben-Othman, J. (2014). Detecting greedy behavior by linear regression and watchdog in vehicular ad hoc networks. In *2014 IEEE Global Communications Conference* (pp. 5032-5037). IEEE.

Mejri, M. N., Achir, N., & Hamdi, M. (2016). A new group Diffie-Hellman key generation proposal for secure VANET communications. In *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (pp. 992-995). IEEE.

Mejri, M. N., Ben-Othman, J., & Hamdi, M. (2014). Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communications*, *1*(2), 53-66.

Mershad, K., & Artail, H. (2012). A framework for secure and efficient data acquisition in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, *62*(2), 536-551.

Mishra, B., Nayak, P., Behera, S., & Jena, D. (2011). Security in vehicular adhoc networks: a survey. In *Proceedings of the 2011 International Conference on Communication, Computing & Security* (pp. 590-595). ACM.

Modi, C. N., Patel, D. R., Patel, A., & Muttukrishnan, R. (2012, July). Bayesian Classifier and Snort based network intrusion detection system in cloud computing. In 2012 *Third International Conference on Computing, Communication and Networking Technologies* (ICCCNT'12) (pp. 1-7). IEEE.

Mokhtar, B., & Azab, M. (2015). Survey on security issues in vehicular ad hoc networks. *Alexandria Engineering Journal*, *54*(4), 1115-1126.

Morgan, Y. L. (2010). Notes on DSRC & WAVE standards suite: Its architecture, design, and characteristics. *IEEE Communications Surveys & Tutorials*, *12*(4), 504-518.

Mythili, A & Magendran, S.K. (2018). Clustering Algorithm and Ensemble SVM for Attack Detection in VANET. *International Journal of Pure and Applied Mathematics, 119* (12), 15407-15419.

Nadeem, A., & Howarth, M. P. (2014). An intrusion detection & adaptive response mechanism for MANETs. *Ad Hoc Networks*, *13*, 368-380.

Naik, M. (2015). Early Detection and Prevention of DDOS attack on VANET (Doctoral dissertation).

Nasir, M. K., Hossain, A. D., Hossain, M. S., Hasan, M. M., & Ali, M. B. (2013). Security challenges and implementation mechanism for vehicular ad hoc network. *International Journal Of Scientific & Technology Research*, *2*(4), 156-161.

Navaz, A. S., Sangeetha, V., & Prabhadevi, C. (2013). Entropy based anomaly detection system to prevent DDoS attacks in cloud. *arXiv preprint arXiv:1308.6745*.

Nema, M., Stalin, S., & Lokhande, V. (2014). Analysis of attacks and challenges in VANET. *International Journal of Emerging Technology and Advanced Engineering*, *4*(7), 831-835.

Nguyen, V. L., Lin, P. C., & Hwang, R. H. (2018). MECPASS: Distributed denial of service defense architecture for mobile networks. *IEEE Network*, *32*(1), 118-124.

Oo, T. T., & Phyu, T. (2013). A statistical approach to classify and identify DDoS attacks using UCLA dataset. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *2*(5), 1766-1770.

Osanaiye, O., Cai, H., Choo, K. K. R., Dehghantanha, A., Xu, Z., & Dlodlo, M. (2016). Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. EURASIP Journal on Wireless Communications and Networking, (1), 130.

Pandeeswari, N., & Kumar, G. (2016). Anomaly detection system in cloud environment using fuzzy clustering-based ANN. *Mobile Networks and Applications*, 21(3), 494-505.

Panjeta, S., Aggarwal, E. K., & Student, P. G. (2017). Review paper on Different Techniques in Combination with IDS. *International Journal of Engineering Science*, *11623*.

Patel, N. J., & Jhaveri, R. H. (2015). Trust based approaches for secure routing in VANET: a survey. *Procedia Computer Science*, *45*, 592-601.

Pathan, A. S. K. (Ed.). (2016). *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press.

Pathre, A., Agrawal, C., & Jain, A. (2013). A novel defense scheme against DDOS attack in VANET. In *Wireless and Optical Communications Networks (WOCN), 2013 Tenth International Conference on* (pp. 1-5). IEEE.

Pavan, K., Sarma & Lokanatha, R. (2019). Classification of DDOS Attacks in VANETs based on distributive dollaborative framework. *International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8*(6).

Poongodi, M., Hamdi, M., Sharma, A., Ma, M., & Singh, P. K. (2019). DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET. *IEEE Access*, *7*, 183532-183544.

Raiya, R., & Gandhi, S. (2014). Survey of various security techniques in VANET. *International Journal of Advanced Research in Computer Science and Software Engineering*, *4*(6)

Rajesh, K. D & Shanmugam, A. (2016). Energy efficient and trust based black hole attack identification model in wireless sensor networks. *Journal of Network Security Computer Networks,* 2(3)

Raju, M. J., Subbaiah, P., & Ramesh, V. (2013). A novel elliptic curve cryptography based aodv for mobile ad-hoc networks for enhanced security. *Journal Of Theoretical & Applied Information Technology*, *58*(3)

Rampaul, D., Patial, R. K., & Kumar, D. (2016). Detection of DoS Attack in VANETs. *Indian Journal of Science and Technology*, *9*(47)

Rasheed, A., Gillani, S., Ajmal, S., & Qayyum, A. (2017). Vehicular ad hoc network (VANET): A survey, challenges, and applications. In Vehicular Ad-Hoc Networks for Smart Cities (pp. 39-51). Springer, Singapore.

Rasheed, A., Gillani, S., Ajmal, S., & Qayyum, A. (2017). Vehicular ad hoc network (VANET): A survey, challenges, and applications. In *Vehicular Ad-Hoc Networks for Smart Cities* (pp. 39-51). Springer, Singapore.

Rawal, B., Ramcharan, H., & Tsetse, A. (2013). Emergence of DDoS resistant augmented Split architecture. In *2013 High Capacity Optical Networks and Emerging/Enabling Technologies* (pp. 37-43). IEEE.

Raya, M., & Hubaux, J. P. (2005). The security of vehicular ad hoc networks. In *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks* (pp. 11-21). ACM.

Razvodovsky, Y. E. (2016). The effect of gorbachevs anti-alcohol campaign on road traffic accidents mortality in belarus. *Journal of Alcoholism & Drug Dependence*

Razzaque, M. A., Salehi, A., & Cheraghi, S. M. (2013). Security and privacy in vehicular ad-hoc networks: survey and the road ahead. In *Wireless Networks and Security* (pp. 107-132). Springer, Berlin, Heidelberg.

Reddy, J. B., Deneire, L., Van der Perre, L., Gyselinckx, B., & Engels, M. (2000). On equalization for OFDM-dedicated short-range communication (DSRC) modem. In *2000 IEEE International Conference on Personal Wireless Communications. Conference Proceedings (Cat. No. 00TH8488)* (pp. 230-234). IEEE.

RoselinMary, S., Maheshwari, M., & Thamaraiselvan, M. (2013). Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA). In *2013 international conference on information communication and embedded systems (ICICES)* (pp. 237-240). IEEE.

Ross Jr, H. E., Sicking, D. L., Zimmer, R. A., & Michie, J. D. (1993). *Recommended procedures for the safety performance evaluation of highway features* (No. 350).

S. A. A. Shah, E. Ahmed, M. Imran, S. Zeadally. (2018). 5G for vehicular communications. *IEEE Communications Magazine*, *56*(1), 111-117.

Sabouni, R., & Hafez, R. M. (2012). Performance of DSRC for V2V communications in urban and highway environments. In *2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)* (pp. 1-5). IEEE.

Sahare, K. B., & Malik, L. G. (2014). An approach for detection of attack in VANET. *International Journal of Engineering Research and Applications ,*23-29

Sahi, A., Lai, D., Li, Y., & Diykh, M. (2017). An efficient DDoS TCP flood attack detection and prevention system in a cloud environment. *IEEE Access*, *5*, 6036-6048.

Sailaja, P., Ravi, B., & Jaisingh, T. (2018). Performance analysis of AODV and EDAODV routing protocol under congestion control in VANETs. In *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)* (pp. 945-948). IEEE.

Sangulagi, P., Sarsamba, M., Talwar, M., & Katgi, V. (2013). Recognition and Elimination of Malicious Nodes in Vehicular Ad hoc Networks (VANET's). *Indian Journal of Computer Science and Engineering,* 4(1).

Sari, A., Onursal, O., & Akkaya, M. (2015). Review of the security issues in vehicular ad hoc networks (VANET). *International Journal of Communications, Network and System Sciences*, *8*(13), 552.

Saritha, V., Krishna, P. V., Misra, S., & Obaidat, M. S. (2017, May). Learning automata based optimized multipath routing using leapfrog algorithm for VANETs. *In 2017 IEEE International Conference on Communications (ICC)* (pp. 1-5). IEEE.

Schweitzer, N., Stulman, A., Margalit, R. D., & Shabtai, A. (2016). Contradiction based gray-hole attack minimization for ad-hoc networks. *IEEE Transactions on Mobile Computing*, *16*(8), 2174-2183.

Shafi, S., Bhandari, B. N., & Ratnam, D. V. (2018). A cross layer design for efficient multimedia message dissemination with an adaptive relay nodes selection in VANETs. In *Conference on Signal Processing and Communication Engineering Systems* (SPACES) (pp. 81-84). IEEE.

Dietzel, S., Petit, J., Heijenk, G., & Kargl, F. (2012). Graph-based metrics for insider attack detection in VANET multihop data dissemination protocols. *IEEE Transactions on Vehicular Technology*, *62*(4), 1505-1518.

Seuwou, P., Patel, D., Protheroe, D., & Ubakanma, G. (2012). Effective security as an ill-defined problem in vehicular ad hoc networks (VANETs).

Shabbir, M., Khan, M. A., Khan, U. S., & Saqib, N. A. (2016). Detection and prevention of distributed denial of service attacks in VANETs. In *Computational Science and Computational Intelligence (CSCI),* (pp. 970-974). IEEE.

Shah, S. A. A., Ahmed, E., Imran, M., & Zeadally, S. (2018). 5G for vehicular communications. *IEEE Communications Magazine*, *56*(1), 111-117.

Shakshuki, E. M., Kang, N., & Sheltami, T. R. (2013). EAACK—a secure intrusion-detection system for MANETs. *IEEE Transactions on industrial electronics*, *60*(3), 1089-1098.

Sharma, N., & Mukherjee, S. (2012). Layered approach for intrusion detection using naïve Bayes classifier. In *Proceedings of the International Conference on Advances in Computing, Communications and Informatics* (pp. 639-644). ACM.

Sharma, S., & Sharma, S. (2017). A novel mechanism of detection of sybil attack in VANETS using timestamp approach. *Int. J. Innovations Eng. Technol*, *8*(1), 200-204.

Singh, A., & Sharma, P. (2015, December). A novel mechanism for detecting DoS attack in VANET using Enhanced Attacked Packet Detection Algorithm (EAPDA). In *2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS)* (pp. 1-5). IEEE.

Singh, S., & Agrawal, S. (2014). VANET routing protocols: Issues and challenges. In *2014 Recent Advances in Engineering and Computational Sciences (RAECS)* (pp. 1-5). IEEE.

Sinha, A., & Mishra, S. K. (2013). Preventing vanet from dos & ddos attack. *International Journal of Engineering Trends and Technology* (IJETT), *4*(10), 4373-4376.

Sinha, A., & Mishra, S. K. (2014). Queue Limiting Algorithm (QLA) for Protecting VANET from Denial of Service (DoS) Attack. *International Journal of Computer Applications, 86*(8), 14-17.

Sinha, A., & Mishra, S. K. (2013). Preventing VANET From DoS & DDOS Attack. *International Journal of Engineering Trends and Technology (IJETT), 4(10)*, 4373-4376.

S'nchez-Casado, L., & García-Teodoro, P. (2012). An efficient cross-layer approach for malicious packet dropping detection in MANETs. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 231-238). IEEE.

Su, M. Y. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Computer Communications*, *34*(1), 107-117.

Sudheera, K. K., Ma, M., Ali, G. M. N., & Chong, P. H. J. (2016). Delay efficient software defined networking-based architecture for vehicular networks. In *2016 IEEE International Conference on Communication Systems (ICCS)*(pp. 1-6). IEEE.

TamilSelvan, K. S., & Rajendiran, R. (2013). A holistic protocol for secure data transmission in VANET. *International Journal of Advanced Research in Computer and Communication Engineering*, *2*(6), 2278-1021.

Tangade, S. S., & Manvi, S. S. (2013). A survey on attacks, security and trust management solutions in VANETs. In *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)* (pp. 1-6). IEEE.

Tanuja, K., Sushma, T. M., Bharathi, M., & Arun, K. H. (2015). A survey on VANET technologies. *International Journal of Computer Applications*, *121*(18).

Thai, M. T., Xuan, Y., Shin, I., & Znati, T. (2008). On detection of malicious users using group testing techniques. In *2008 The 28th International Conference on Distributed Computing Systems* (pp. 206-213). IEEE.

Thang, T. M., & Nguyen, V. K. (2016). Synflood Spoof Source DDoS Attack Defence based on Packet ID anomaly Detection-PIDAD. In *Information Science and Applications (ICISA) 2016* (pp. 739-751). Springer, Singapore.

Theresa, W. G., & Sakthivel, S. (2017). Fuzzy based intrusion detection for cluster-based battlefield MANET. In *2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)* (pp. 22-27). IEEE.

Tonkin, S. L., McIntosh, C. G., Hadden, W., Dakin, C., Rowley, S., & Gunn, A. J. (2003). Simple car seat inserts to prevent upper airway narrowing in preterm infants: A pilot study. *Pediatrics*, *112*(4), 907-913.

Tyagi, P., & Dembla, D. (2014). Investigating the security threats in vehicular ad hoc networks (VANETs): Towards security engineering for safer on-road transportation. In *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 2084-2090). IEEE.

Vaibhav, A., Shukla, D., Das, S., Sahana, S., & Johri, P. (2017). Security challenges, authentication, application and trust models for vehicular ad hoc network-a survey. *IJ Wireless and Microwave Technologies*, *3*, 36-48.

Van, N. T., Thinh, T. N., & Sach, L. T. (2017). An anomaly-based network intrusion detection system using deep learning. In *2017 International Conference on System Science and Engineering (ICSSE)* (pp. 210-214). IEEE.

Verma, K., & Hasbullah, H. (2015). Bloom-filter based IP-CHOCK detection scheme for denial of service attacks in VANET. *Security and Communication Networks, 8*(5), 864-8

La Hoa, V., & Cavalli, A. (2014). Security attacks and solutions in vehicular ad hoc networks: a survey. *Int. J. Netw. Syst, 4*(2)

Vipin, D., & Chhillar, R. S (2018) The DDOS Attack Detection and Prevention in VANET by group controlled analysis model. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),* 7 (3)

Wagan, A. A., & Jung, L. T. (2014). Security framework for low latency VANET applications. In *2014 International Conference on Computer and Information Sciences (ICCOINS)* (pp. 1-6). IEEE.

Wang, P., Wu, L., Cunningham, R., & Zou, C. C. (2010). Honeypot detection in advanced botnet attacks. *International Journal of Information and Computer Security*, *4*(1), 30-51.

Wang, W., & Gombault, S. (2008). Efficient detection of DDoS attacks with important attributes. in *Third International Conference on Risks and Security of Internet and Systems*. doi:10.1109/crisis.2008.4757464

Wasef, A., Lu, R., Lin, X., & Shen, X. (2010). Complementing public key infrastructure to secure vehicular ad hoc networks security and privacy in emerging wireless networks. *IEEE Wireless Communications*, *17*(5), 22-28.

Williams, B. (2008). *Intelligent transport systems standards*. Artech House.

Xiang, M., Chen, Y., Ku, W. S., & Su, Z. (2011). Mitigating DDOS attacks using protection nodes in mobile Ad hoc networks. In *2011 IEEE Global Telecommunications Conference-GLOBECOM 2011* (pp. 1-6). IEEE.

Xiang, Y., Liu, Z., Liu, R., Sun, W., & Wang, W. (2013). GeoSVR: A map-based stateless VANET routing. *Ad Hoc Networks*, *11*(7), 2125-2135.

Xu, J., Tang, X., & Lee, W. C. (2006). Time-critical on-demand data broadcast: Algorithms, analysis, and performance evaluation. *IEEE Transactions on parallel and distributed systems*, *17*(1), 3-14.

Yan, G., Rawat, D. B., & Bista, B. B. (2012). Towards secure vehicular clouds. In *2012 Sixth International Conference on Complex, Intelligent, and Software Intensive Systems* (pp. 370-375). IEEE.

Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2015). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Communications Surveys & Tutorials*, *18*(1), 602-622.

Yaqoob, I., Ahmad, I., Ahmed, E., Gani, A., Imran, M., & Guizani, N. (2017). Overcoming the key challenges to establishing vehicular communication: Is SDN the answer? *IEEE Communications Magazine, 55*(7), 128-134.

Yin, J., Holland, G., Elbatt, T., Bai, F., & Krishnan, H. (2006). DSRC channel fading analysis from empirical measurement. In *2006 First International Conference on Communications and Networking in China* (pp. 1-5). IEEE.

Zaidi, K., & Rajarajan, M. (2015). Vehicular internet: Security and privacy challenges and opportunities. *Future Internet*, *7*(3), 257-275.

Zeadally, S., Hunt, R., Chen, Y. S., Irwin, A., & Hassan, A. (2012). Vehicular ad hoc networks (VANETS): Status, results, an Signature-Based Detection Approaches d challenges. *Telecommunication Systems*, *50*(4), 217-241.

Zeng, Y., Qiu, M., Ming, Z., & Liu, M. (2018). Senior2Local: A machine learning based intrusion detection method for vanets. In *International Conference on Smart Computing and Communication* (pp. 417-426). Springer, Cham.

Zhang, Y., Zhao, J., & Cao, G. (2010). Service scheduling of vehicle-roadside data access. *Mobile Networks and Applications*, *15*(1), 83-96.

Zhibin, W. (2007). Network Simulator 2 for Wireless. Retrieved from http://www.winlab.rutgers.edu/~zhibinwu/html/network_simulator_2.html

Zhong, R., & Yue, G. (2010, April). DDoS detection system based on data mining. In *Proceedings of the 2nd International Symposium on Networking and Network Security, Jinggangshan, China* (pp. 2-4).

Zhu, H., Lu, R., Shen, X., & Lin, X. (2009). Security in service-oriented vehicular networks. *IEEE Wireless Communications*, *16*(4), 16-22.