An Intelligent Intrusion Detection System for External Communications in Autonomous Vehicles

By

Khattab M. Ali

A thesis submitted for the degree of ***Doctor of Philosophy***

School of Computer Science and Electronic Engineering

University of Essex

2017

Abstract

Advancements in computing, electronics and mechanical systems have resulted in the creation of a new class of vehicles called autonomous vehicles. These vehicles function using sensory input with an on-board computation system. Self-driving vehicles use an ad hoc vehicular network called VANET. The network has ad hoc infrastructure with mobile vehicles that communicate through open wireless channels. This thesis studies the design and implementation of a novel intelligent intrusion detection system which secures the external communication of self-driving vehicles. This thesis makes the following four contributions:

It proposes a hybrid intrusion detection system to protect the external communication in self-driving vehicles from potential attacks. This has been achieved using fuzzification and artificial intelligence. The second contribution is the incorporation of the Integrated Circuit Metrics (ICMetrics) for improved security and privacy. By using the ICMetrics, specific device features have been used to create a unique identity for vehicles. Our work is based on using the bias in onboard sensory systems to create ICMetrics for self-driving vehicles.

The incorporation of fuzzy petri net in autonomous vehicles is the third contribution of the thesis. Simulation results show that the scheme can successfully detect denial-of-service attacks. The design of a clustering based hierarchical detection system has also been presented to detect worm hole and Sybil attacks. The final contribution of this research is an integrated intrusion detection system which detects various attacks by using a central database in BusNet. The proposed schemes have been simulated using the data extracted from trace files. Simulation results have been compared and studied for high levels of detection capability and performance. Analysis shows that the proposed schemes provide high detection rate with a low rate of false alarm. The system can detect various attacks in an optimised way owing to a reduction in the number of features, fuzzification.

This work is dedicated to

My Parents (Mr. & Mrs. ***Maajal)***

*My Dear Wife (****Suhad****), and*

*My Lovely Daughters (****Lana & Dana****)*

Acknowledgements

First, my thanks and gratitude should be expressed to Almighty Allah who has granted me patience and spiritual support in my life.

I would love to have the opportunity to say thank you for all those who have a hand in the completion of this research work. I am deeply grateful to my supervisor **Prof. Klaus McDonald-Maier** whose help and suggestions were never-ending and valuable over the course of writing this thesis. I would also like to express my sincere thanks to the staff of School of Computer Science and Electronic Engineering, as well as the staff of the library who have provided the excellent atmosphere of study during the time of writing up my thesis.

Thanks to the Iraqi Government represented by the Ministry of Higher Education and Scientific Research and University of Anbar for the financial support and for giving me the opportunity to undertake this experience.

My sincere thanks should also go to my colleagues Shoaib Ehsan, Anna Gruebler and Hasan Tahir who helped me during the practical application for my project. They really have provided me with penetrating ideas and suggestions.

I should not forget my family. My sincere and special thanks to my dearest wife. She has actually provided me with encouragement and support over the period of study in the United Kingdom. Her love, patience and support removed all the difficulties that I had to face.

A word of thanks and indebtedness should also be mentioned for my parents. In spite of the difficult life in my country they have been and are still with me with their continuous support. My mother who has always been with me with her prayers, spiritual support and assistance. And my father who has given me everything in my life. Words stand mute in front of them.

Keywords

Intrusion Detection Systems, Self-Driving Vehicles, Semi Self-Driving Vehicles, Fuzzy Petri Net, Security, Artificial Neural Networks, Support Vector Machine, k-Nearest Neighbours

Contents

Chapter One – Introduction

Chapter Two – Theoretical Background and Literature Survey

Chapter Three – Intrusion Detection System for Autonomous Vehicles

Chapter Four - An Intrusion Detection Scheme for Self-Driving Vehicles Based on ICMetrics Techniques

Chapter Five - Fuzzy Intrusion Detection System and Intelligent Response Systems for Autonomous Vehicles

Chapter Seven - Conclusion and Future Directions

Bibliography

List of Figures

List of Tables

List of Abbreviations

Abbreviation	***Details***
ADCCP	Advanced Data Communication Control Protocol
AES	Advanced Encryption Standard
AGT	Application Layer
ANN	Artificial Neural Network
AODV	Ad Hoc On Demand Distance Vector
AP	Application Attack
Application Programming Interface	API
ARAN	Authenticated Routing for Ad hoc Networks
ART	Attack-Resistant Trust
AWK	Alfred Aho, Peter Weinberger and Brian Kernighan
B-MFR	Border based Most Forward within Radius
BSM	Basic Safety Message
BusNet	Bus Network Layer
BusNet-IDS	Bus Network Intrusion Detection System
CA	Certificate Authority
CAMs	Cooperative Awareness Messages
CAN	Control Area Network
CBR	Constant Bit Rate
CF	Confidence Degree Factor
CH	Clustering-Head
CityMob	City Mobility
CMs	Cluster Members
CSER	Cooperative Security-Enforcement Routing
CVHAS	Cooperative Vehicle-Highway Automation Systems
D	Dropped action

DDoS	Distributed Denial-of-Service
DM	Downtown Model
DoS	Denial-of-Service
DPR	Drop Packet Rate
DSR	Dynamic Source Routing
ECUs	Electronic Control Units
e-Maps	Electronic Maps
f	forward action
FCC	Federal Communications Commission
FFNN	Feed-Forward Neural Network
FN	False Negative
FP	False Positive
FPN	Fuzzy Petri Net
GPS	Global Positioning System
GPSR	Greedy Perimeter Stateless Routing
HDLC	High-Level Data Link Control
HMM	Highway Mobility Model
ICMetrics	Integrated Circuit Metrics
ID	Identity
IDSs	Intrusion Detection Systems
IP	Internet Protocol
IPS	Intrusion Prevention System
IQR	Inter Quartile Range
ITS	Intelligent Transport System
IVC	Inter-Vehicular Communications
KDD	Knowledge Discovery and Data Mining
kNN	k Nearest Neighbours
LDA	Linear Discriminant Analysis
LIN	Local Interconnect Network
MAC	Media Access Control
MANETs	Mobile Ad Hoc Networks
MEMS	Micro-Electro Mechanical Systems

MFR	Most Forward within Radius
MLP	Multilayer Perceptron
MM	Manhattan Model
MOST	Media Oriented Systems Transport
MOVE	Mobility Vehicles
NAM	Network Animator
ns-2	Network Simulator Version Two
OBUs	On Board Units
OOP	Object Oriented Programming
OTCL	Object Tool Command Language
PBSRP	Position Based Secure Routing Protocol
PDR	Packet Delivery Rate
POS	Proportional Overlapping Score
PPP	Point-to-Point Protocol
Privacy-Preserving Detection of Abuses of Pseudonyms	P2DAP
PTSM	Probabilistic Traffic Sign
PUF	Physically Unclonable Functions
QDA	Quadratic Discriminant Analysis
QoS	Quality of Service
r	received action
RACE Integrity Primitives Evaluation Message Digest	RIPEMD
RDS	Radio Data System
REPLY	Route Reply
RERR	Route Error
ROS	Resiliency Oriented Secure
RREQ	Route Request
RSA	Rivest-Shamir-Adleman Cryptosystem
RSSI	Radio Strong Signal Integrate
RSUs	Roadside Units
RSUs	Roadside Units

RTR	Routing Layer
RUM	Rice University Model
RWP	Random Way Point
s	send action
SAAR	Security-Aware Ad hoc Routing
SAODV	Secure AODV
SD	Standard Deviation
SEAD	Secure Efficient Ad hoc Distance
SLSP	Secure Link-State Protocol
SM	Simple Model
SOM	Self-Organising Map
RP	Secure Routing Protocol
SSM	Stop Sign Mode
SUMO	Simulation Urban Mobility Model
SVM	Support Vector Machines
TA	Trust Authority
TCL	Tool Command Language
TCP	Transport Control Protocol
TDMA	Time Division Multiple Access
TLM	Traffic Light Model
TN	True Negative
TORA	Temporally Ordered Routing Algorithm
TP	True Positive
TPD	Tamper-Proof Devices
TPMS	Tire Pressure Monitoring System
TTP	Trusted Third Party
TTP	Trust Third Party
UAVs	Unmanned Aerial Vehicles
UDP	User Datagram Protocol
UDP	User Data Protocol
UUVs	Unmanned Underwater Vehicles
V	Vehicle

V2I	Vehicular to Infrastructure
VANETs	Vehicular Ad Hoc Networks
V-AODV	Vehicle Ad Hoc On Demand Distance Vector
Verity Level	VL
VID	Vehicle Identification
WHO	World Health Organisation
WLAN	Wireless Local Area Network Protocols

CHAPTER ONE

INTRODUCTION

"The beginning of knowledge is the discovery of something we do not understand."

Frank Herbert (1920-1986)

Autonomous systems play a significant role in developing and deploying modern technology [1]. These systems such as self-driving vehicles, robots, Unmanned Underwater Vehicles (UUVs) and Unmanned Aerial Vehicles (UAVs), have contributed significantly to scientific research, wars, reconnaissance and intelligence [1]. Furthermore, they have had a direct and positive impact on promoting and supporting the scientific revolution.

According to the statistics of many international organisations, such as World Health Organisation (WHO), more than 1.24 million people die in road accidents every year all over the world, in addition to 20 to 30 million nonfatal injuries [2]. The number of deaths and injuries is expected to increase by 65% in the next two decades [3]. These figures of deaths and injuries are caused by the drivers' mistakes (human errors) through driving and travelling on the roads [4]. These problems are intended to be fixed by one of the applications of the autonomous systems, which is autonomous vehicles, sometimes also called self-driving, driverless or robotic vehicles [5].

1.1 Driverless Vehicles

Autonomous or robotic vehicles (for example, Google's driverless vehicle) are considered one of the most significant applications of autonomous systems and that provides the main motivation for this thesis. These vehicles can promote the safety of road users, whether drivers or passengers, and they can also have many positive economic impacts on society [6]. They have the ability to reduce the number of accidents and traffic jams on busy roads. In addition, one economic benefit of these self-driving vehicles is the ideal use of the narrow roads through the application of the platoon behaviour [6]. Figure 1.1 below explains the platoon in self-driving vehicles. Hence, they can establish safety environment for passengers, drivers and vehicles themselves. Primarily, three key technologies are needed to enable autonomous or semi-autonomous vehicles to function: an embedded processor, an array of sensors and a communication system (internal and external) [1].

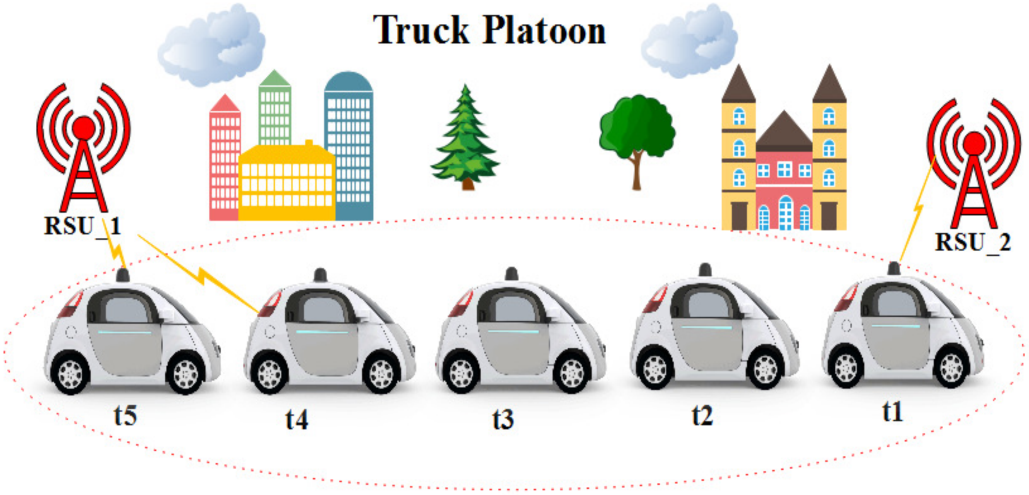


Figure 1.1 Platoon in Autonomous Vehicles.

Self-driving and semi-autonomous vehicles depend largely on communication systems, whether internal or external, to predict events and sense their external environment used in their moves. The moving/stopping decision of vehicles depends on data and information that is collected by the sensors and from On-Board Units (OBU).

In addition, these communication systems enable autonomous vehicles to achieve their goals, such as traffic management, reducing the number of deaths and injuries from traffic accidents on busy roads, reduce human errors and achieve the ideal exploitation of available resources [7]. In other words, the autonomous vehicles can achieve their tasks without human intervention [8]. These vehicles need wireless communication systems to connect vehicles with each other and with their infrastructure on the road side. This network enables the vehicles to exchange necessary information, warning notification, data control and Cooperative Awareness Messages (CAMs).

All studies have shown that the external communication system used in self-driving or semi-autonomous vehicles are vehicular ad hoc networks (VANETs) [9], [10], [11]. The VANETs are mobile nodes that allow vehicles to communicate with each other in a particular zone as well as with Road Side Units (RSUs) in the absence of a fixed security infrastructure that is used in traditional networks such as a wired network [12]. In addition, VANETs are considered a subclass or subtype of mobile ad hoc networks (MANETs) [13]. They have a direct influence on the Intelligent Transportation Systems (ITS) by providing safety applications and comfort services to drivers and passengers. The goal of VANETs is to provide safety to road users and the vehicles themselves. Hence, VANETs are vital now and in future as it eliminates time and space constraints and makes information available when required for autonomous vehicles [14]. These networks can achieve their goals via an exchange of CAMs, control data, and they provide comfort and emergency notifications to passengers and drivers, such as messages regarding emergency braking or accidents [15], [16]. Furthermore, the networks have the most critical role in self-driving and semi-autonomous vehicles.

1.1 Driverless Vehicles

VANETs are exposed to many security and privacy problems because of their unique characteristics that distinguish them from other wireless networks, such as high dynamic topology, the enormous number of vehicles on roads, open medium wireless communication, speed, lack of traditional fixed security stations and high mobility [17]. Unfortunately, the VANETs are exposed to many attacks, such as network, application and social attacks. Moreover, these security problems are reflected directly and negatively on the performance of self-driving and semi-autonomous vehicles.

The VANETs create new threats to self-driving and semi-autonomous vehicles that contribute to substantial challenges in autonomous systems. These communication systems render driverless vehicles vulnerable to many types of attacks, such as Denial-of-Service (DoS), black hole, grey hole, dropping and flooding, wormhole and Sybil attacks [18].

Recently, research has revealed that the external communication systems in self-driving and semi-autonomous vehicles have experienced problems with these security and privacy systems [19], [20]. Thus, it is anticipated that there will be a gradual increase in the number of security and privacy problems with these vehicles. Hence, the autonomous vehicles will be exposed to new security issues unless significant changes to the security design of autonomous vehicles are made. There is substantial scientific evidence that current security mechanisms are not sufficient or efficient enough to protect the external communications employed in self-driving vehicles [21].

Employing VANETs in autonomous vehicles makes the success of this new generation of technology dependent on the security of the networks. Today, security in most systems is based on the concept of defence in depth, as is the use of multiple layers of defences to prevent adversaries from violating security policies of these systems. Intrusion Detection Systems (IDS) offer a second layer of defence for the

VANETs [22]. Intrusion detection techniques focus on the detection/identification of malicious activity that normally is an attacker. It is able to penetrate the system and steal sensitive data such as velocity, position and identification (ID).

Despite the application of the security approaches, including access control and authentication services to improve the protection of the networks, these defence mechanisms alone are not sufficient to deter and block all types of attacks, especially internal attacks in VANETs. They are still in need of additional protection systems, such as IDS, to increase their security.

In this thesis, a novel intelligent intrusion detection system is proposed which can protect the external communication of self-driving and semi-autonomous vehicles from any potential attacks. Although, the proposed security systems have the ability to detect and block internal and external attacks, they would have a direct and adverse impact on the performance of these vehicles.

The proposed IDS uses the features extracted from the networks auditable data which has been generated in a network simulator. The proposed IDS utilises two types of detection - anomaly based detection and misuse based detection to detect malicious behaviour. A hybrid IDS is designed and implemented to detect different of attacks on VANETs. The proposed IDSs in this thesis are composed into six parts. This thesis studies the design and implementation of the individual parts of the intrusion detection systems. These combined components aim to improved the security of autonomous vehicles.

The first part: IDS is based on the features extracted from trace file that has been generated from the network simulator version two (ns-2) to detect the malicious vehicle. It has the ability to identify four types of attacks: DoS, black hole, grey hole and rushing. In this proposed IDS, artificial intelligence techniques are employed in designing the security system, such as Feed-Forward Neural Network (FFNN), Support Vector Machine (SVM), k-Nearest Neighbours (k-NN), Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA).

The second part: The proposed IDS uses the latest Integrated Circuit Metric (ICMetrics) technology to detect both internal and external attacks on external communications in self-driving and semi-autonomous vehicles. The ICMetrics technology uses internal features of a vehicle to generate an identification called an ICMetric. It can be used to provide services related to authentication and attack detection. The ICMetrics generation is an automated process and does not need user intervention. It is generated when required and discarded there after, thus reducing the chances of identity perversion.

The third part: Fuzzy Petri Net (FPN) is utilised in designing an intelligent IDS to secure the communication system of driverless and semi-autonomous vehicles. The proposed detection system is based on the interval of beacons (time) that is generated from the vehicles in the platoon behaviour. It is usually considered one of the most important aspects of a new generation of vehicles. In the platoon, the vehicles create a convoy which has many benefits such as reducing cost and enhancing connection performance. FPN-IDS is considered a novel detection system because this is the first time an FPN is employed in designing an intelligent security system for VANETs.

The fourth part: Mobile-IDS is proposed to secure the external communication system for autonomous vehicles. It is based on a virtual layer to sniff or eavesdrop data and information that is sent/transferred between vehicles and RSUs to detect different types of DoS attacks, such as flooding and drooping. The proposed IDS was installed on buses to detect abnormal/ malicious behaviour and it was also introduced in an urban area.

The fifth part: The distributed IDS is based on a Trusted Third Party (TTP) that functions like a data-centric scheme which registers the position, time and ID for each vehicle on roads to enable detection of Sybil attacks. In addition, Sybil attack is a leading cause of many types of other attacks, such as node impersonation and fabrication attacks. In other words, the distributed IDS can detect/identify Sybil, impersonation and fabrication attacks.

The sixth part: Integrated-IDS has the ability to detect various types of attacks on the external communication system of self-driving and semi-autonomous vehicles, such as black hole, grey hole, rushing, flooding, dropping and Sybil attacks. It is based on the position of vehicles and interval beacons that are generated from the vehicles to detect impersonation, Sybil and DoS attacks. To increase the defensive capability of the proposed IDS, it is integrated on a RSU.

All the proposed intelligent security systems have demonstrated good performance in detecting and blocking the malicious vehicle in VANETs of self-driving vehicles and semi-autonomous vehicles. At least one research paper for each part was published in international conferences and journals. We have formulated a clear research question:

How can we detect an intruder quickly and effectively in the communication networks of self-driving and semi-autonomous vehicles*?*

A novel quick reaction mechanism, programmed inside the data link layer of the network that enters the victim vehicle in the safe mode, is designed for infected self-driving and semi-autonomous vehicles. The mechanism will allow the infected vehicles to communicate directly with the nearby RSU without any intermediary at a suitable time without delay. In other words, when the infected vehicle is unable to connect with neighbouring vehicles in any situation, the vehicles will directly connect to the closest infrastructure on the roadside, for example, the RSU. The safe mode response provides superior response capabilities with improved performance.

Finally, routing protocols influence the efficiency of detection and the selection of stable routers in VANETs. Ad Hoc On Demand Distance Vector (AODV) is used in the proposed schemes because it is considered one of the most important protocols in ad hoc networks [23]. The basic AODV has been adapted to reduce communication overhead and enhance the stability of selected route between source and destination vehicle. The proposed AODV protocol, formally called Vehicle AODV (V-AODV), is effort to improve the network performance by incorporating new routing selection algorithm.

1.2 Motivation

Self-driving and semi-autonomous vehicles are, of course, a great addition to ITS. These vehicles try to improve traffic management and provide safety environment to the passengers/drivers. In other words, the target of the autonomous vehicles is to improve security of passengers and drivers by reducing the number of road accidents and traffic jams caused by human error [21]. Current research shows that the communication systems in self-driving vehicles have encountered problems with the security and privacy systems [1], [2], [8]. The external communication system of self-driving vehicles inherits security weakness of ad hoc networks. In addition, new security challenges are added to self-driving vehicles because of their unique features of the external communication system, such as fast change topology, and an enormous number of vehicles. The proposed IDSs in this thesis address security and privacy issues for the communication system of self-driving vehicles. To sum up, without significant changes to the security design of the autonomous vehicles, we will see a gradual increase in the number of security attacks on these vehicles. There is enough evidence that the current security measures are insufficient to protect the external communication systems for self-driving and semi-autonomous vehicles [22]. The security system, economic impact, safety and privacy are considered key motivations in this thesis. The motivation in this thesis is based on the four following factors:

1) *The Security Factor*. The application of VANETs in autonomous vehicles makes the success of this new generation of technology dependent on the security of the networks. Despite the use of the protection approach, including access control and authentication services to improve the security of the networks, these defence mechanisms alone are not sufficient to deter all types of attacks. The security system of self-driving vehicles needs to have some properties such as being lightweight, robust, fast and efficient and capable of online-detection.
2) *The Economic Factor*. Driverless vehicles are considered one of the most significant applications of autonomous systems. Platoon behaviour of these vehicles plays a vital role in reducing costs through the ideal use of narrow roads. In this case, these vehicles enable the largest number of vehicles on the narrow roads, and this will have a significant economic impact on the expansion of the road [24].
3) *The Attacks Type Factor.* Traditional security systems such as encryption mechanisms are unable to detect all types of attacks on the external communication of autonomous vehicles, especially internal attacks in VANETs. They are still in need of backup protection systems, such as IDS, to increase their security.
4) *The Safety Factor*. To save passengers and drivers' lives, self-driving vehicles need to have an intelligent reaction response system which has the ability to introduce an infected vehicle into a safe mode immediately and without delay.

Machine learning has the ability to generate meaning from huge, imprecise and complex datasets [25]. It can be utilised detect class and extract patterns which are very complex. Machine learning techniques can be employed for some applications that are not possible to solve for humans or other computer technologies. The machine learning techniques are employed in this thesis which are: Fuzzy Petri Nets, Artificial Neural Networks, Support Vector Machines, k-Nearest Neighbours, Linear discriminant analysis and Quadratic discriminant analysis. They have some characteristics that distinguish them from other techniques, for example real time operation, fault tolerance, self-organisation and adaptive learning [25]. Various of machine learning techniques are used in this thesis to improve detection rate and reduce the number of false alarms that generated from detection process for our proposed security systems. Traditional systems are often unable to make decisions with significant amounts of data at critical time [26]. In this case, machine learning schemes can play important role in make optimal decision at short time.

1.3 Thesis Challenges

A wide range of safety, non-safety applications, traffic management, security and privacy systems have been established for future deployment in external communication of self-driving and semi-autonomous vehicles [27]. However, these security systems and services applications faced many challenges that were considered obstacles to developing the VANETs. The high mobility, and dynamic change in network topology are considered the most challenging issues in developing and deploying communication systems of autonomous vehicles [11], [28].

1.3.1 Communication System Challenges

The external communication system of self-driving vehicles has characteristics which distinguish it from other networks. Unfortunately, these characteristics also present technical and security challenges for the deployment of self-driving vehicles. These challenges can be classified into the following categories [28]:

1) *Network Management*. The high dynamic change topology, high mobility, velocities make network management a very difficult task in VANETs. In addition, the enormous number of vehicles and rapid channel changing add extra challenges to VANETs management.
2) *Communication Environment.* Wireless communication in VANETs creates new threats for security systems in the external communication of autonomous vehicles. Hence, attackers can launch attacks from anywhere and anytime without physical access. This communication environment makes designing and building secure communication systems for self-driving vehicles a challenging and complicated task.
3) *Environmental Impact.* Electromagnetic waves are utilised in the principle communication system of vehicles. The external environmental factors play an important and direct role in the performance of VANETs. In addition, buildings and mountains have a substantial impact on the quality and strength of the broadcast signal.
4) *Congestion and Collision Control.* The congestion and collision occur in VANETs when the traffic load is very high that makes communication difficult between vehicles, and with RSUs in that radio coverage area. This challenge has a direct and adverse impact on the performance metrics of VANETs, such as decreasing the amount of Packet Delivery Ratio (PDR) and increasing the amount of dropping packets.

1.3.2 Security Challenges

The distinguishing process between normal and abnormal/malicious behaviour is one of the most complicated issues in VANETs because of the dynamically changing topology and the volatile physical environment. The security challenges can be classified into following categories [14]:

1.3 Thesis Challenges

1) *Online Detection*. Real-time detection is one of the critical issues in designing security systems. In safety applications, CAMs and data control should arrive at the destination node with 100*ms* transmission delay. At this point, the intelligent detection system should have the ability to identify and allow sent/received packets between source and target at the suitable time without delay. Any delay will have a direct impact on the life of passengers and drivers.
2) *High Mobility*. The detection system is based heavily on features that have been collected from network behaviour. Moreover, the high mobility in VANETs makes the collection process for type and number of features very difficult. As a result, the designers of security systems need to some technologies to fill the gap that is created by high mobility in VANETs, such as fuzzification.
3) *Traditional Security Systems.* The conventional security systems are unable to provide sufficient security to the communication system of self-driving vehicles. In this case, VANETs need to design and build a new security system or modify existing protection systems.
4) *Internal Attacks.* All encryption algorithms can detect and prevent the external attacks. Unfortunately, these algorithms are unable to prevent internal attacks that have a negative effect on VANETs. This encourages researchers to create and find security systems which can detect and prevent attacks on VANETs such as intelligent IDS.

These challenges should be taken into account of designers to avoid problems that were caused in creating security obstacles. In this thesis, a novel intrusion detection system is proposed to overcome these key challenges.

1.4 Problem Statement

Communication systems are considered one of the fundamental components in the development and existence of autonomous systems, such as driverless vehicles. Research has shown that autonomous vehicles have encountered problems with the security of their communication systems [1]. Moreover, the use of ad hoc wireless networks for these vehicles has added new threats as they have increased the vulnerability of the communication systems [29]. Vehicular communication differs from other wireless communication networks because of the high mobility involved and the rapidly changing topology that makes security a huge challenge in self-driving vehicles. Protection of these networks and the creation of new security mechanisms will increase the development and promotion of autonomous vehicles [30].

VANETs have incorporated some of the characteristics that have made them susceptible to many security attacks. These properties are [31]:

- An open communication medium.
- A highly changeable topology.
- Cooperative communication algorithms.
- The absence of fixed security infrastructures.
- Lack of centralised point whether management, defence and monitoring.
- High mobility.

Unfortunately, such characteristics represent the vulnerabilities of the VANETs which make them easy to penetrate by the attacker. The security of these networks is vital as, in the case of malicious behaviour involving just one vehicle, the entire system will be paralysed which will affect all other vehicles in that particular zone, for example via DoS attacks. These attacks will prevent communication between all the vehicles in that radio coverage area. The deployment and evolution of self-driving vehicles are dependent on providing security for all the system components. One such component is the communications system.

1.5 Thesis Aim and Objectives

The aim of the invention of self-driving vehicles is to reduce the number of accidents and traffic jams caused by human errors on busy traffic roads. These vehicles cannot predict the road conditions so they need to be able to exchange data and CAMs with other vehicles and with RSUs. In other words, the movements and actions of self-driving vehicles depend heavily on the data control and sensitive information that are collected from the external environment (gained information). In this scenario, the accuracy of the data exchanged between vehicles and RSUs has a significant role and will directly influence the lives of passengers, drivers and the vehicles themselves [30]. One of the most critical issues is the protection of the data control and the data transferred between these vehicles.

This thesis aims is to provide intelligent intrusion systems to secure the external communication systems (VANETs) to be used in self-driving and semi-autonomous vehicles. In addition, the proposed intrusion detection has the ability to protect data and warning messages that are exchanged between vehicles and RSUs. For this purpose, we introduce more than one intelligent IDS to secure the external communication system of these vehicles from the potential attacks. The aim is to secure sent/transferred data and CAMs between the source and the destination from any expected attacks.

The proposed security system must be able to detect and block various attacks such as DoS, Sybil, flooding, black hole, grey hole, dropping, wormhole and rushing attacks in self-driving and semi-autonomous vehicles.

In this thesis, the objectives are as follows:

1.5 Thesis Aim and Objectives

- Designing an intelligent IDS to secure the external communication system of autonomous and semi-autonomous vehicles.
- Training and testing the proposed IDS using optimised Feed-Forward Neural Network (FFNN), Support Vector Machine (SVM), k-Nearest Neighbours (k-NN), Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA).
- Designing an IDS with different detection schemes and architectures.
- Employing some of the techniques that are used for the first time in building IDS such as FPN and Proportional Overlapping Score (POS) in selecting significant features.
- Detecting and blocking a range of external and internal attacks on self-driving and semi-autonomous vehicles and network.
- Developing a time-efficient system so that the safe mode can be induced in a compromised vehicle without delay. In other words, designing and implementing a quick response for abnormal scenarios in VANETs.
- Implementing the detection system using various routing protocols.
- Creating mobility and traffic model to generate trace file to detect abnormal scenarios.
- Enhancing performance detection which is increasing detection rate and reducing the number of false alarms by declining the number of features that have been extracted from trace file and Kyoto dataset.
- Fuzzification, normalisation and uniform distribution of significant features extracted from trace file by using POS method.
- Comparison and analysis of the results to show improved detection rates in false alarms.

1.6 Thesis Contributions

In this thesis, various intelligent IDSs are proposed to secure the external communication of self-driving and semi-autonomous vehicles. The proposed security system has the ability to protect the data control and sensitive information that are sent/transferred between vehicles and RSUs in that radio coverage area. A knowledge basis is incorporated into this thesis to detect and block different types of potential attacks on the communication system. In addition, artificial intelligence techniques are utilised in building and improving the performance of IDS. The major contributions are outlined below:

1.6.1 Designing Intrusion Detection System

- Designing various intelligent IDSs to secure the external communication system for self-driving and semi-autonomous vehicles such as FFNN-IDS, SVM-IDS, LDA-IDS, QDA-IDS, k-NN-IDS, BusNet-IDS and Distributed-IDS.
- Designing IDSs with different detection algorithms, architectural models and artificial intelligence techniques to get different detection mechanisms with different performance metrics values.
- ICMetrics technology is employed in designing novel ICMetric-IDS to secure vehicles communication systems. It is based on readings bias collected from different sensors, such as accelerometer, gyroscope, magnetometer and ultrasonic sensors, which are utilised in designing IDS.
- Proposing a novel IDS based on FPN. This is the first time FPN is utilised in building IDS for VANETs. It is based on features that are calculated from trace file such as PDR and Drop Packet Rate (DPR).

- Designing hybrid “anomaly and misuse” based-detection methods to overcome their limitations. In other words, we make use of the benefits of both types of detection systems by designing hybrid IDS.
- Designing integrated-IDS to identify various attacks, such as black hole, grey hole, wormhole, Sybil. These attacks influence the performance of IDS.
- IDS is installed on vehicles and RSUs to provide full safety environment for self-driving and semi-autonomous vehicles. The proposed IDS is designed using three architectural styles i.e. stand-alone, cooperative and hierarchical.
- Finally, external and internal attacks are detected and blocked by the proposed intelligent IDS.

1.6.2 Improving the Performance of the Detection System

- Enhancing detection rate and reducing the amount of false alarms that is generated from the proposed IDS. In this thesis, the goal is to get the best results by using some techniques, such as fuzzification, normalisation, uniform distribution, sub-validation dataset and POS, to select significant features.
- Creating a new dataset to evaluate performance for the proposed IDS from the trace file that is generated by ns-2. To generate real traffic and mobility environment for self-driving vehicles, the ns-2 utilises two software which are: Simulation of Urban Mobility Model (SUMO) and Mobility Vehicles (MOVE).
- Reducing the number of extracted features to improve detection performance. The elimination of useless features improves the detection rate, decreases the computation time and memory consumption, and hence enhancing the overall performance of an IDS
- The Kyoto data set is used to validate detection performance for the proposed IDS. Significant features are selected from Kyoto dataset to reduce the computation time and memory consumption.

1.6.3 Designing a Novel Response System

- Designing a novel response system to introduce infected vehicles in safe mode at a suitable time without delay to save the life of passengers and drivers.
- Improving the authentication aspect of self-driving and semi-autonomous vehicles by generating an ICMetrics basis number, which is generated from bias reading of typical automotive sensors.

1.7 Thesis Outline

The remainder of this thesis is organised as follows:

Chapter Two presents the literature review associated with security of self-driving vehicles. The chapter particularly focuses on intrusion detection algorithms and methods being utilised in VANETs. In Chapter two, an overview of communication systems for self-driving vehicles is provided, as well as threats and vulnerability in the external communication system for autonomous vehicles. In addition, the relevant artificial intelligence techniques, detection types and routing protocol employed are reviewed in this chapter. Moreover, the security goals are discussed that should be taken into account when building intrusion detection system.

Chapter Three proposes more than one IDS to detect and block various attacks such as, DoS, black hole, grey hole, rushing attacks. In addition, methodologies, artificial intelligent technologies, mobility and traffic models that are employed in the design of intrusion detection system are reviewed.

Chapter Four presents the novel intrusion detection system based on readings bias that have been extracted from various sensors in self-driving vehicles. The intrusion detection system uses the latest ICMetrics technology to secure data control and sensitive information from potential attacks. Then, it detects both internal and external attacks on external communication system of autonomous vehicles.

In **Chapter Five**, a new response reaction mechanism is proposed to transfer the infected vehicle into safe mode at a suitable time to save the life of passengers and driver, as well as vehicles themselves. The safety model is integrated with a novel intrusion detection system that is based on FPN. This is the first time FPN is utilised in building IDS for VANETs.

In **Chapter Six**, an integrated-IDS has been proposed to create a practical and robust system for self-driving vehicles. The proposed security system is created by merging two approaches i.e. BusNet-IDS and the distributed-IDS. By composing two security solutions the resulting system can detect a range of attacks like flooding, drooping, impersonation, fabrication and Sybil attacks. In the proposed design, the content of a message is determined by selecting one of the two integrated IDS approaches i.e. BusNet-IDS or distributed-IDS.

Finally, the conclusions are presented in **Chapter Seven.** Some ideas for future work are also discussed in this chapter.

1.8 List of Publications

This thesis is based on the following recent publications. These papers are divided into four categories:

1.8.1 Published

I. **K. M. Ali Alheeti**, A. Gruebler, K. McDonald-Maier: Using Discriminant Analysis to Detect Intrusions in External Communication of Self-Driving Vehicles, Published in the Elsevier Digital Communications and Networks (DCN) Journal, volume: 3, issue:3, pp: 180-187, 2017.

II. **K. M. Ali Alheeti**, K. McDonald-Maier: An Intrusion Detection Scheme for Driverless Vehicles Based Gyroscopic Sensor Profiling, Proceedings of the 35th

IEEE International Conference on Consumer Electronics (ICCE), pp. 448-449, Las Vegas – USA, January 2017.

III. **K. M. Ali Alheeti**, K. McDonald-Maier: An Intelligent Security System for Autonomous Cars based on Infrared Sensors, Proceedings of the 23rd IEEE International Conference on Automation and Computing (ICAC'17), Huddersfield, UK, September 2017.

IV. **K. M. Ali Alheeti,** E. Shoaib, K. McDonald-Maier: An Enhanced AODV Protocol for External Communication in Self-Driving Vehicles, Proceedings of the 7th IEEE International Conference on Emerging Security Technologies (EST), Canterbury, UK, September 2017.

V. Rabab Al-Zaidi, John Woods, Mohammed Al-Khalidi, **K. M. Ali Alheeti** and K. McDonald-Maier: Ship Ad Hoc Networks in a Maritime Environment: Imperatives, Challenges and Realization, Proceedings of the 2nd International Conference on Fog and Mobile Edge Computing (FMEC), Valencia, Spain, May 2017

VI. **K. M. Ali Alheeti**, A. Gruebler, K. McDonald-Maier: Prediction of DoS Attacks in External Communication for Self-Driving Vehicles Using a Fuzzy Petri Net Model, Proceedings of the 34th IEEE International Conference on Consumer Electronics (ICCE), pp. 502-503, Las Vegas, USA, January 2016.

VII. **K. M. Ali Alheeti**, K. McDonald-Maier: Hybrid Intrusion Detection in Connected Self-Driving Vehicles, Proceedings of the 22nd IEEE International Conference on Automation and Computing (ICAC'16), pp: 456 – 461, Colchester, UK, September 2016.

VIII. [1]**K. M. Ali Alheeti**, A. Gruebler, K. McDonald-Maier: Intelligent Intrusion Detection of Grey Hole and Rushing Attacks in Self-Driving Vehicular Networks, Published in the MDPI Computers Journal, Computers 5, no. 3, 2016.

IX. **K. M. Ali Alheeti**, K. McDonald-Maier: An Intelligent Intrusion Detection Scheme for self-driving Vehicles Based Magnetometer Sensor, Proceedings of the IEEE International Conference for Student on Applied Engineering (ICSAE) Conference Newcastle, pp: 75 – 78, UK, September 2016.

X. **K. M. Ali Alheeti**, Anna Gruebler, K. McDonald-Maier: On the Detection of Grey hole and Rushing Attacks in Self-Driving Vehicular Networks, Proceedings of the 7th IEEE International Conference on Computer Science and Electronic Engineering Conference (CEEC), pp. 231-236, Colchester, UK, September 2015.

XI. **K. M. Ali Alheeti**, A. Gruebler, K. McDonald-Maier: An Intrusion Detection System Against Black Hole Attacks on the Communication Network of Self-Driving Cars, Proceedings of the 6th IEEE International Conference on Emerging Security Technologies (EST), pp. 86-91, Brunswick, Germany, September 2015.

XII. **K. M. Ali Alheeti**, A. Gruebler, K. McDonald-Maier: An Intrusion Detection System Against Malicious Attacks on the Communication Network of Driverless Cars, Proceedings of the 12th IEEE International Conference on Consumer Communications Networking Conference (CCNC), pp. 916-921, Las Vegas, USA, January 2015.

XIII. **K. M. Ali Alheeti**, S. Ehsan, K. McDonald-Maier: An Assessment for Recent Attacks on Specific Embedded Systems, Proceedings of the 5th IEEE International Conference on Emerging Security Technologies (EST), pp: 88 – 93, Alcala de Henares, Spain, September 2014.

[1] This paper was also selected as a featured article out of 45 papers published in that particular issue (MDPI Computer Journal). This paper is designated as highly accessed.

XIV. **K. M. Ali Alheeti**, L. Al-Jobouri, K. McDonald-Maier: Increasing the Rate of Intrusion Detection based on a Hybrid Technique, Proceedings of the 5th IEEE International Conference on Computer Science and Electronic Engineering Conference (CEEC), pp: 179 – 182, Colchester, UK, September 2013.

XV. **K. M. Ali Alheeti**, K. McDonald-Maier: Intelligent Intrusion Detection for Autonomous Vehicles, Published in the Systems Science and Control Engineering Journal.

XVI. [2]**K. M. Ali Alheeti,** K. McDonald-Maier: A Hierarchical Detection Method in External Communication for Self-Driving Vehicles Based on TDMA, Published in the PLOS one Journal.

1.8.2 Under Self- Review

I. **K. M. Ali Alheeti**, K. McDonald-Maier: Employing Fuzzy Petri Net for The Detection of Attacks on External Communication in Self-Driving and Semi Self-Driving Vehicles, we will submit to the PLOS one Journal.

II. **K. M. Ali Alheeti**, K. McDonald-Maier: An Intrusion Detection Scheme for Self-Driving Vehicles Based on ICMetric Technical, we will submit to the IEEE Sensors Transaction Journal.

1.8.3 In Draft

I. **K. M. Ali Alheeti**, K. McDonald-Maier: On the Utilization of BusNets in Vehicular Ad hoc Network Security, we will submit to the IEEE Vehicular Technology Magazine.

II. **K. M. Ali Alheeti**, K. McDonald-Maier: Sybil Node Detection and Localisation in VANETs for Self-Driving Vehicles, we will submit to the POLS one.

[2] This journal has 2.806 Impact Factor.

CHAPTER TWO

THEORETICAL BACKGROUND AND LITERATURE SURVEY

"It is a capital mistake to theorize before one has data. Insensibly one begins to twist facts to suit theories, instead of theories to suit facts"

Arthur Conan Doyle, Sherlock Holmes

Traditional security systems do not have the ability to protect sensitive information or control data of communication systems or host computers from internal attacks [32]. Cryptographic and digital signature techniques are considered as traditional security systems and the first layer/line of defence [33]. They are based on public key cryptography, symmetric encryption and hash functions which can secure systems/networks against external attacks [33]. Attack countermeasures can be utilised to reduce the attack possibilities [34]. Moreover, these techniques are built for a set of known attacks and they are unable to prevent new attacks [34]. In addition, these techniques are unable to protect systems/networks from internal/insider attacks when the attacker knows or gets the private/public keys. The attackers use keys to perform encryption/decryption processes. For these reasons, the external communication system in autonomous vehicles needs a second security layer to "detect and notify". i.e., "intrusion detection system" (IDS).

Here, an IDS can help to detect and block internal and external attacks on those systems that are considered the second layer of security system, such as encryption/decryption. The external communication system of autonomous vehicles has an increased vulnerability compared to other networks, such as wired networks, as there are no stationary security infrastructures. Moreover, a high dynamic topology network and the open wireless medium makes them more vulnerable to attack [35].

2.1 Autonomous Vehicles

Autonomous vehicles are considered one of the important applications in autonomous systems. These vehicles play a vital role in enhancing transport approaches by reducing the number of accidents are caused by human errors. Google has had a big role in the development of self-driving vehicles and has seen great success through logging of more than 500,000 miles without any incidents [36]. Here, we can summarise the potential safety benefits of autonomous vehicles: 1.24 million people were killed on the roads in 2010 in 180 countries [2]. In the United States, there were 5.4 million accidents; as a result of these accidents, more than 32,885 people were killed and injured more than 2.2 million injured in 2010 [37]. The cost of accidents in 2009 the was more than $299.5 billion [38]. Studies show that more than 5.471 of accidents in 2005-2007 were 92.3% from the mistakes of drivers [39]. All these facts and error statistics have encouraged to produce a new generation of vehicles, the self-driving vehicles, because this type of vehicles can avoid driver's errors.

Although it is a complex technology, it mainly consists of four components: sensors, mapping, perception, and communication system [40].

1. Sensor devices: Vehicles contain of a number of sensors used in the perception of the external environment, such as infrared, radar, GPS, accelerometer and gyroscope, LiDAR and cameras.

- Infrared sensors: Used at night for the detection of animals and other vehicles.
- Radar sensors: Used for measuring the range and velocity of self-driving vehicles.

- Global Positioning Systems (GPS): Used for determining the position. Some recent studies advise not to use this device due to the inaccuracies in the GPS data [41].
- Accelerometers and gyroscopes: used to identify changes in the speed and directions.
- LiDAR: This is one of the most expensive sensors, which is used in autonomous vehicles, using lasers and photoreceptor to produce a three-dimensional model of the surrounding environment.

2. Mapping, usually use files containing points and lines of the road, origin and destination entities, photographic images from the streets of satellites, ground pictures from the streets, as well as traffic control devices and obstacles. The mapping may contain the forms of terrain that were obtained by LiDAR.
3. Perception is a set of programs that combines data from various sensors and compares the input data with the stored data. It is responsible for maintaining and determining the vehicle's position with traffic lines, monitoring and responding to traffic control devices, pedestrians, and other obstacles on the roads. The perception keeps track of the vehicle location with maps. Finally, it monitors the health of vehicles and automated systems.
4. Communication is a very important thing in the self-driving vehicles. According to the United States Department of Transportation (USDOT), communication reduces the number of accidents by 80 percent [42]. The communication technology is sometimes called the (connected vehicle) [42], [43] or (Cooperative Vehicle-Highway Automation Systems (CVHAS)) [44].

Self-driving vehicles pose challenges for those planning and designing transportation facilities. Here are a few examples which show the potential problems [40]:

- Platooning: It is the form which represents self-propelled vehicles in movement on roads, sometimes called (road trains) [45]. This phenomenon posed that self-driving vehicles need transmission lines and distances, especially for the purpose of separating or joining by other vehicles.
- Loading, unloading, and parking: parking areas must be re-designed to be able to accommodate a larger number of passengers. These parking spaces may be far from the landing areas of passengers.
- Lane widths and pavement design: these vehicles will exploit corridors optimally allowing us to narrow the lines of transportation, but we need to re-design the pavement.
- Rules of the road: the roads are going to be a mixture of self-driving vehicles and manual. In this case, self-driving vehicles must mimic the behaviour of the driver in the movement.
- Regional traffic volumes: when self-driving vehicles are allowed to run on the roads, the fundamental nature of the travel will change.
- Goods movement and public transportation: vehicles for the transport of goods need to queue for loading or unloading.

To bypass the testing phase of self-driving vehicles must pave the way to overcome some of the obstacles [12]:

- Critical Mass: These vehicles need transmitter and receiver, and this should provide the service on all vehicles for the success of this technique.
- Infrastructure Modifications: communication vehicle infrastructure need to be built, but the cost may be a challenge to implement this project. The compromise is to focus only on the big critical intersections to avoid accidents. Another solution is to use the current cellular networks with infrastructure. Cellular networks have problems with speed (slow) and a low bandwidth.

- Dependency on Sensors.

Our research focuses on providing intelligent security systems to protect external communication systems in self-driving vehicles from the potential attacks due to their importance and effective role in the emergence of this generation of vehicles.

2.2 Communication Infrastructure for Autonomous Vehicles

Communication systems are an essential component in the success of autonomous vehicles. There are two types of communication systems: external and internal communication system infrastructure. Figure 2.1 demonstrates external communication scenarios in autonomous vehicles.

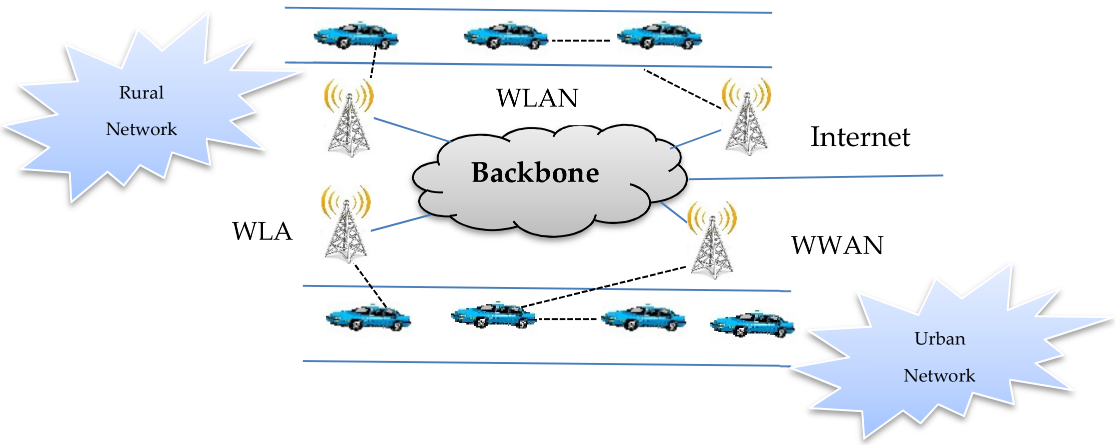


Figure 2.1 External Communication of Autonomous Vehicles.

The Media Access Control (MAC) protocol relies upon vehicles in communication. This protocol includes a variety of Wireless Local Area Network (WLAN) protocols, such as the IEEE 802.11 [46]. There were some necessary amendments to the IEEE 802.11 protocol to support the exchange of data between vehicles. The IEEE 802.11 is used to produce the new protocol, which is IEEE 802.11p. This protocol has remained under development. It has not been applied and only used for the purposes of testing.

2.2 Communication Infrastructure for Autonomous Vehicles

Vehicular ad hoc network relies on short-range wireless communications between vehicles, for example, Dedicated Short Range Communication (DSRC) [47] and IEEE 802.11 [48].

Generally, there are two types of communication in VANETs [30]:

- Inter-Vehicular Communications (IVC): Autonomous vehicles equipped with communication devices are usually short-range. These vehicles can exchange information within the radio waves. This kind of networking is known as a VANET. Low cost and ease of deployment are some of the important features of this network.
- Communication between the vehicle and the infrastructure (V2I) is used for the purpose of monitoring traffic and management services.

2.2.1 External Communication Infrastructure

Autonomous vehicles need information, which is present in other vehicles. In this case, they must be provided with broadband communications to access external resources. For example, these communications enable the passenger to communicate with others (people) and access local services such as tourist information, traffic information, gas stations and restaurants [49].

2.2.1.1 Attacks on External Communication Infrastructure (VANETs)

VANETs are prone to many different types of attacks that lead to greater challenges in protection. Cooperation awareness messages transmitted among vehicles should be routed through routing protocols. This information will be exposed to many attacks.

Attacks can be classified depending on the source of the attack internal/ inside and external/ outside. An external attacker is going to insert, re-send or distort messages, while the internal attacker is inside the network. It broadcasts false information to other vehicles. Detection of these messages that carry false information will be very difficult because these malware vehicles can create legal signatures using their private keys. These types of external attacks will cause direct harm to the routing information. Firewall and encryption mechanisms are common measures to get rid of this type of attack.

In addition, attacks can be classified as active or passive [29]. A passive attack is a type of attack which monitors or analyses data traffic that is sent among vehicles, or controls the traffic flow by eavesdropping. Whereas active attack is a type of attack which causes damage to the network by modifying the data and sends back the previous messages that causes a denial-of-service.

Researchers describe the various types of attacks through their studies [50], [51], [52] and [53] and categorise them in four classes:

1. **Network Attacks**: The main components of the VANET are vehicles and infrastructure. This type of attack has a direct impact on the vehicle and the infrastructure. These attacks also have a high priority because of their impact on the whole network. The main goal of the attackers is to create problems for legitimate users and network. Some of the attacks are mentioned below:
    - **Denial-of-Service (DoS) Attack:** availability in the networks of vehicles is considered very important for the fact that all users depend on the communication network.
    - **Distributed Denial-of-Service (DDOS) Attack:** it is considered one of the most dangerous attacks in vehicle environments due to the fact that these attacks are distributed.
    - **Sybil Attack**: this kind of attack is considered a network attack [54]. These attackers send multiple messages to other vehicles, and each message contains a different fabricated source identity (ID). It can give, for example,

the illusion of a traffic jam to other vehicles by sending wrong messages [55].

- **Node Impersonation Attack:** each vehicle has a unique number of VANET networks used for the verification of messages. The attackers try to send wrong messages to other vehicles [55], [56].
- One of the attacks suffered by these networks is a **Wormhole attack**, where the attacker can capture packets from one location and tunnel them to another location. This will make the wormhole between the legitimate nodes of the network.

2. **Application Attack (AP)**: vehicles need two types of applications, which are safety and non-safety. The main concern of this attack is to change the content of these applications for their interests. Safety application is very important in vehicle networks since they provide warning messages to other users. The attackers try to change the content of the messages and send the wrong ones. This may cause accidents. One of the examples of this attack is Bogus [50]. This attacker sends false messages to the network, which causes users to change their behaviour on the road. Warning, caution and notification messages are considered one of the important messages of safety applications.
3. **Timing Attack**: this is a new type of attack which adds a time slot to the original messages and creates a delay. This type of attack does not change the content of messages, but creates a kind of delay leading to its late receipt. Time is important in safety applications and delayed alarm messages can cause accidents on the road.
4. **Social Attack:** All immoral messages are social attacks. The purpose of this attack is to send indirect messages, which aim at creating problems in a network. These messages have an unethical influence on the behaviour of

drivers on the road. For instance, a driver may receive a message, "you are an idiot", which may make the driver increase the speed to catch up with the sender of this message. This will indirectly affect other users in the network.

2.2.2 Internal Communication Infrastructure

Vehicles are equipped with computers, communications capabilities and remote sensing to provide necessary information and services to vehicles and passengers. Intelligent Transportation Systems (ITS) were instrumental in the emergence of self-driving vehicles [6].

The major requirements for any vehicle to be in VANETs are: An On Board Units (OBUs) that contain a processor, memory, GPS unit, transceiver, sensors, antenna and communication modules. Most of the modern vehicles are equipped with all these to support VANETs [57].

Embedded electronic components in modern vehicles called Electronic Control Units (ECUs), are considered an important part of the architecture of vehicles. The responsibility of these systems is to monitor and control different subsystems of the vehicle, interconnected through internal networks [58].

With a large number of electronic control units in vehicles, it is difficult to connect two electronic control units directly (point to point) since linking directly requires extra cost and space. They can be interrelated with each other through a bus, and they send messages to all associated nodes. To correlate them, we need several protocols. Thus, vehicles made up of several sub-networks continue among themselves through an electronic control unit gateway. These networks are [58]:

- **Control Area Network** (CAN) is a serial bus designed for vehicles. Data rate is 1Mbps. If there is more than one node that wants to send a message at the same time of the electronic control units.

- **Local Interconnect Network** (LIN): This type of network uses the principle of master-slave. Messages are sent from the slave after a request from the master at a rate of 20kbps. This protocol is inexpensive, but the rate of data transmission is low.
- **FlexRay**: The advantage of this protocol is the large data-transfer rate (10Mbps). Due to the cost in the industry, it is used in critical function only.
- **Media Oriented Systems Transport** (MOST): It is used to transmit multimedia through optical fibres. These networks are used to control the channels though which any node sends or receives. Synchronous data channels are used to transport the stream of data at high rates, (24Mbps).

Modern vehicles are now more connected with the outside world via wireless interfaces. They are even enabled to contact other vehicles or the infrastructure. Now, internal networks in vehicles are complemented by external networks to perform tasks. When the vehicle is a closed network, the attacker cannot achieve his attack only by the physical access to the vehicle by cutting the wires, but the vehicles have become open to the outside world. Thus, the threat of attacks is from a remote computer.

2.2.2.1 Attacks on Internal Communication Infrastructure

Attacks on internal communication system of self-driving vehicles have been classified as follows: indirect physical access, short-range wireless access and long range wireless access (direct and indirect) [58].

1. **Indirect Access**: Focuses on third-party attacks that will be at a later time able to attack the vehicle.
    - **OBD Port**: The attacker can use the diagnostic port to attack the vehicle. The attacker can connect a **pass thru** device to the OBD port through Wi-Fi, which works remotely (via a laptop) [59]. Vulnerabilities in communications

Application Programming Interface (API) enables the attacker to achieve his attack remotely (computer). Using this mechanism, the attacker can achieve another attack on the other device sharing the same Wi-Fi.

- **CD Player**: two vulnerabilities are distinguished in this subsection [59]. First, the inclusion of a disk (CD) containing the firmware updates, but in fact it contains a malicious code. Second, decoding of the WMA file may help broadcast messages over the bus for the internal network.
- **USB Port**: vehicle media player can access a corrupted file stored on a USB key.

2. **Short Range Attacks**

These attacks use short-range wireless networks. It is possible that this attack has a direct attack by targeting the vehicle's communication, or indirectly through the driver's devices that are usually connected to the vehicle such as smart phones.

- **Wireless Pairing of Mobile Devices**: modern vehicles can be coupled with mobile devices. For example, a driver can join the mobile phone with the vehicle via Bluetooth. Exploitation of these vulnerabilities may lead to the retrieval of data stored in communications, eavesdropping on the conversation between the passengers and the driver, and in the worst possible scenario, it could take over control of the electronic control unit.
- **Car-to-Car Communications**: Communication between two vehicles or between vehicle and infrastructure is very important in the exchange of information. The attacker can eavesdrop through this or send fake data.
- **TPMS (Tire Pressure Monitoring System)**: This consists of pressure sensors inside the tires, which send their data to an electronic control unit via the radio frequency emitter. The attacker can eavesdrop on these signals and send false signals from 40 meters to the electronic control unit and, thus, illuminate the alarm light.

- **Wireless Unlocking**: A lot of vehicles have the technology to open doors remotely. Encryption is applied to these signals, which are transmitted through the air, thus exposing it to signal violations.

3. **Long-Range Direct Attacks**:

   The attacks are from a remote location.

   - **Telephony**: detection of several vulnerabilities in the telematics unit. Some of the attacks are sent through the 3G network.
   - **Web browsing**: vehicles have a web browser that creates a threat through the injection of malware.

4. **Long Range Indirect Attacks**:

   This kind of attack is from a remote location and indirect (Mediator).

   - **App Store**: using such stores to download programmes is possibly to be harmful since the store might be exposed to attacks, such as a Trojan Horse.
   - **Side Channel Triggers**: broadcast signals of a certain Radio Data System (RDS) constitute a danger to the electronic control units.

2.3 Autonomous Vehicles: Types of Applications

The applications of VANETs are divided into three categories which are: safety, security and infotainment [60]. Autonomous vehicles need two types of applications related to the safety, and efficiency of traffic which depend on the exchange of information between vehicles or between vehicles and roadside units (RSUs) [61]. For the autonomous vehicles to be connected, they must be equipped with computer technology and wireless communication devices, which is referred to as informatics. The main objective of VANETs is to provide safety for passengers [62].

These networks provide three types of applications, which are very important for autonomous vehicles [63]:

- Safety applications are one of the most important applications which are responsible for the warning messages such as an Intersection Collision Warning, Post-Crash Warning, Emergency Electronic Brake Lights and Road Condition Warning. These applications have a significant role in preserving the life of the driver and passengers as well as the vehicle itself.
- Traffic Management Applications: These applications make an ideal driving of self-driving vehicles through the sharing of information between vehicles and with the infrastructure, such as Congested Road Notification, Parking Availability Notification and Parking Spot Locator.
- Commercial Applications: these applications provide comfort and satisfaction to the passengers and drivers, such as service announcements and map download.

2.4 Vehicular Ad hoc Network in Self-Driving Vehicles

Generally, ITS consists of two main parts: Information processing application system and Road condition information transferring system [64]. The responsibility to exchange information between the vehicles, or vehicles with road side units, is of road condition information transferring system [64]. The main aim of VANETs is to provide security and safety for passengers and drivers as well as the vehicle itself [65]. The self-driving vehicles heavily depend on VANETs, making these networks interesting for researchers. These networks provide the security and comfort for the vehicles through cooperative awareness messages which include various applications. A significant increase in the number of vehicles makes driving difficult and dangerous, thus raising the importance of VANETs. In addition, its design or dissemination is low cost compared to other networks.

There are several applications for VANETs, such as Vehicle collision warning, Security distance warning, Driver assistance, Cooperative driving, Cooperative cruise control, Dissemination of road information, Internet access, Map location, Automatic parking, Driverless vehicles [65]. In addition, communication between the vehicles is used to support the achievement of safety-critical services, such as collision warning, up to date traffic and weather information or navigation systems.

2.4.1 Dedicated Short-Range Communication (DSRC)

Dedicated Short Range Communication (DSRC) is considered as short-range wireless protocol which particularly made for V2V and V2I communications in order to enhance the productivity and safety of the transportation system which is also known as ITS. DSRC was originally proposed to work in the 915 MHz band; however, US Federal Communications Commission (FCC) in the year 1999 assigned 75 MHZ of spectrum at 5.9 GHz for DSRC. The same thing also happened in Japan and Europe where 5.8 GHz is used instead for DSRC. The radio technology of DSRC is known to be a variant of the IEEE 802.11a technology [66]. This supplies high data transfer rates which can reach as high as 27 Mbps over a range of 1km while at the same time still maintaining low overhead in the DSRC spectrum. Both academia and industry have been working extensively on standardisation of DSRC. An example of such work is the IEEE P1609 Working Group; the group is currently working on the IEEE802.11p for both MAC and PHY layer of DSRC, including applications and management services over DSRC, which can be referred as Wireless Access in Vehicular Environment (WAVE). The current research highlights (what the research is dealing with in terms of IEEE802.11p) and contributes to the development of the security system as will be discussed in detail in Chapters (3,4, 5 and 6) below.

2.5 Security in Vehicular Ad hoc Networks

The Quality of Service (QoS) is considered an important issue in these networks: delay, throughput, jitter, bandwidth and packet loss, etc. Security is an essential service needed for the secure functioning of VANETs. In other words, security has become one of the major concerns in VANETs. The nature of the VANETs exposed a group of security challenges in the design of these networks. These challenges are the lack of a centralised security infrastructure, participate in open wireless and significant change in topology.

VANETs are more vulnerable to attacks than wired networks. One of the challenges is in the nature of structural VANETs. It is a widely used network. However, after the emergence of a new generation of intelligent vehicles, it has become more important and indispensable for the success of this project. The basic idea applied in MANETs is that it assumes that all nodes in the network are cooperative and there is no malicious node [67]. As VANETs is a subgroup of MANETs based on their work on this idea. Breaching one of the VANETs nodes leads to disruption of the entire network.

The intrusion detection system is one of the protection systems which that are very important in these networks and is a supplement other protection mechanisms, such as encryption. The Intrusion detection system collects and analyses information about the activities of the network, analyse and in the case of detection of any abnormal condition issues an alarm.

The success of the self-driving vehicles relies heavily on its networks and the success of the networks, which depends on the scalability of its security. Generally, the security systems are divided into two parts. Firstly, intrusion prevention systems, such as encryption and authentication (using passwords or biometrics) which is the first layer of defence; intrusion detection techniques ("any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" [68]), is the second layer of defence. Intrusion prevention systems are not sufficient because the systems are becoming more complex.

The concept of security is classified into two classes based on the type of primitive work: proactive and reactive [69]. Protection mechanisms that place restrictions and prevent unauthorised access early, such as encryption, are considered the mechanics of proactive protection; while the mechanisms that detect attacks after the fact and do not put any restrictions like proactive security are reactive, such as IDSs. Figure 2.2 shows the categories of security concepts [69]:

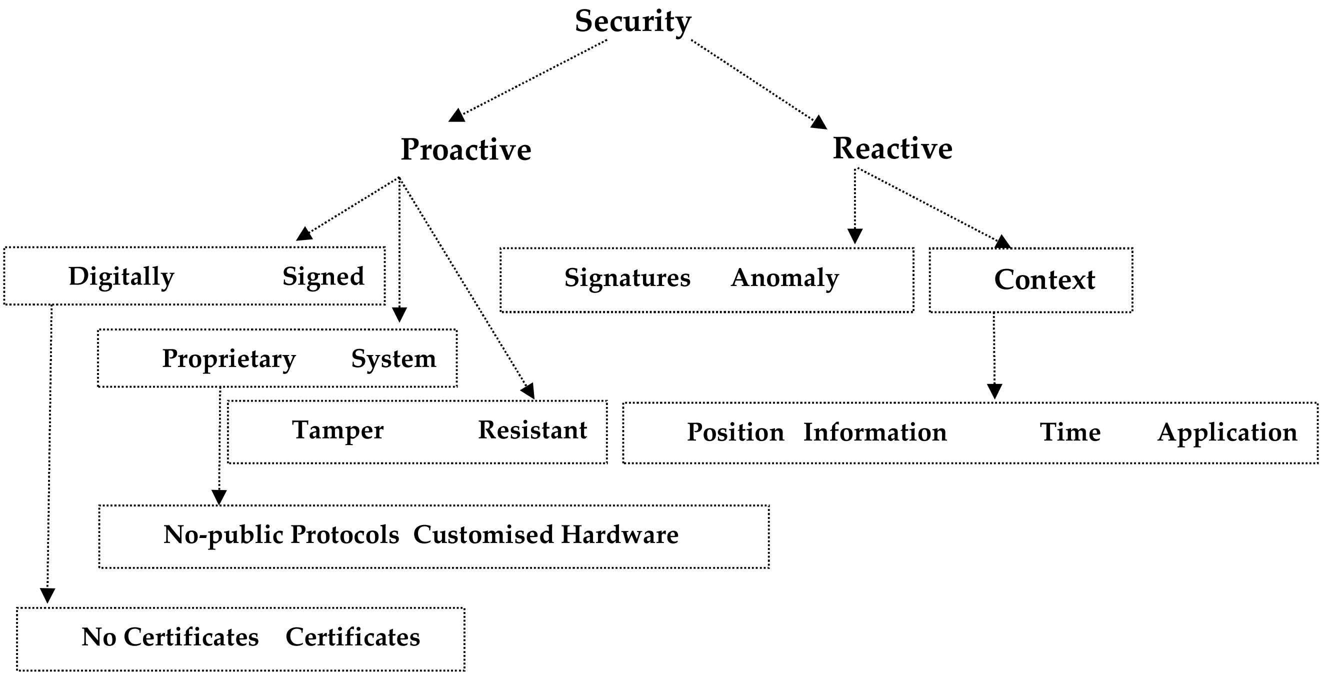

Security
Proactive
Reactive
Digitally Signed
Proprietary System
Tamper Resistant
No-public Protocols Customised Hardware
No Certificates Certificates
Signatures Anomaly
Context
Position Information Time Application

Figure 2.2 Categories of Security Concepts.

Security requirements differ from one system to another, and this depends on the type of system and the main objective of the system design. Security requirements for a system that works in VANETs are [69]:

1. **Timely Delivery**: Time is an important issue and a delay in messages makes them useless.

2. **Location Accuracy and Correctness of Messages**: Location accuracy is also critical. The attacker can exploit this requirement in achieving its objectives by sending more than one message and false information, which confuses the traffic of other vehicles.
3. **Privacy**: Wireless networks make privacy important issue. It must provide a mechanism to protect the data they carry in this message, such as vehicle location, time, speed, and internal vehicles sensor data.
4. **Liability**: This requirement poses some problem as we have to identify who is responsible when the error occurs in the self-driving vehicles.

2.5.1 Targets of Attacks

Vehicular ad hoc networks are exposed to many types of attacks. Some of these attacks are shown in the following subsections. Generally, potential attacks are divided into three categories: the threats against availability, confidentiality and authenticity [70].

1. **Threats on Availability**

Self-driving vehicles rely heavily on their communication (VANETs) with the external environment for make their decisions. Denial-of-service attacks try to take advantage of the opportunity to achieve their objectives in the following two areas [71]:

- Control of a vehicles' resources.
- Jamming the communication channels.

DoS attacks have a direct and negative impact on the life of passengers, drivers and vehicles themselves (when they prevent the arrival of warning/ caution messages to other vehicles) [72], [52] and [73]. The internal or external attacker which has a direct impact on the network by denying users the available resources [74].

This type of attack is the most violent on the VANETs, and is divided into three categories:

a) **Denial-of-Services (DoS)**

- The basic level: Intrusion detection system can detect these attacks and isolate them.
- The extended level: It generates high frequencies to prevent connection. The solution is that the DSRC channel contains seven channels and the vehicle has to switch between these channels to secure the appropriate connection with vehicles or roadside units.

b) **Drop Packet**

- The beacon messages between vehicles are deliberately damaged by malicious vehicle through jamming that launched denial-of-service attacks [75], [76].
- Jamming: It is a type of attack on the physical layer of the network. This attack has direct and negative impact on the platooning phenomenon in self-driving vehicles [77].
- Black hole attack (Remote redirection): The existence of this type of attack causes loss of package (DoS) [78].
- Spamming: This kind of attack does not send messages for consumption the bandwidth of the network and does not pose a risk (advertising messages).

Availability is one of the very important issues in VANETs. Denial-of-service attacker aims to block this feature of these networks. Platooning phenomenon is achieved through the exchange of periodic cooperation messages between vehicles. These messages carry the position and velocity of each vehicle. In the case of blocking, these messages cannot be exchanged between vehicles to achieve this phenomenon, that we refer to as beacons [79]. The danger of this attack is the inability of vehicles to update the information between them.

c) **Message Suppression Attack**

Attackers try to drop packets from the network. They use these packets at other time [52]. These attacks cause a lot of problems and cause many accidents for vehicles on the road.

2. **Threats on Authentication**

The vehicular ad hoc network offers a tradeoff between privacy and authentication that leads to a kind of malicious attack which is Sybil [80]. The networks in the vehicles are exposed to various types of attacks. Such attacks are routing attack (Sybil attacks).

- **Sybil Attacks**: The attacker generates a number of messages with fake IDs that transfer to other vehicles. This is the most lethal attack on the network.
- **Node Impersonation Attack:** each vehicle in the network has a unique number that distinguishes it from the rest of the vehicles. The attacker can change the ID which creates confuse for other vehicles on the roads.
- **Fabrication Attack**: attackers can achieve their goals by broadcasting false messages in the network. These messages are warnings, certificates, Identities [52], [73].

3. **Threats to Integrity**

- **Alteration Attack**: this happens when the attack succeeds in changing the content of the message. Delay or re-sending the message more than once is considered one of the aspects of this attack [52].

Finally, the main existing threats on VANETs are divided into three categories: infotainment application, safety application and secure communications [60]. These threats are summarised in Figure 2.3. In VANET threats, every attack has a direct and negative impact on all types of VANET applications.

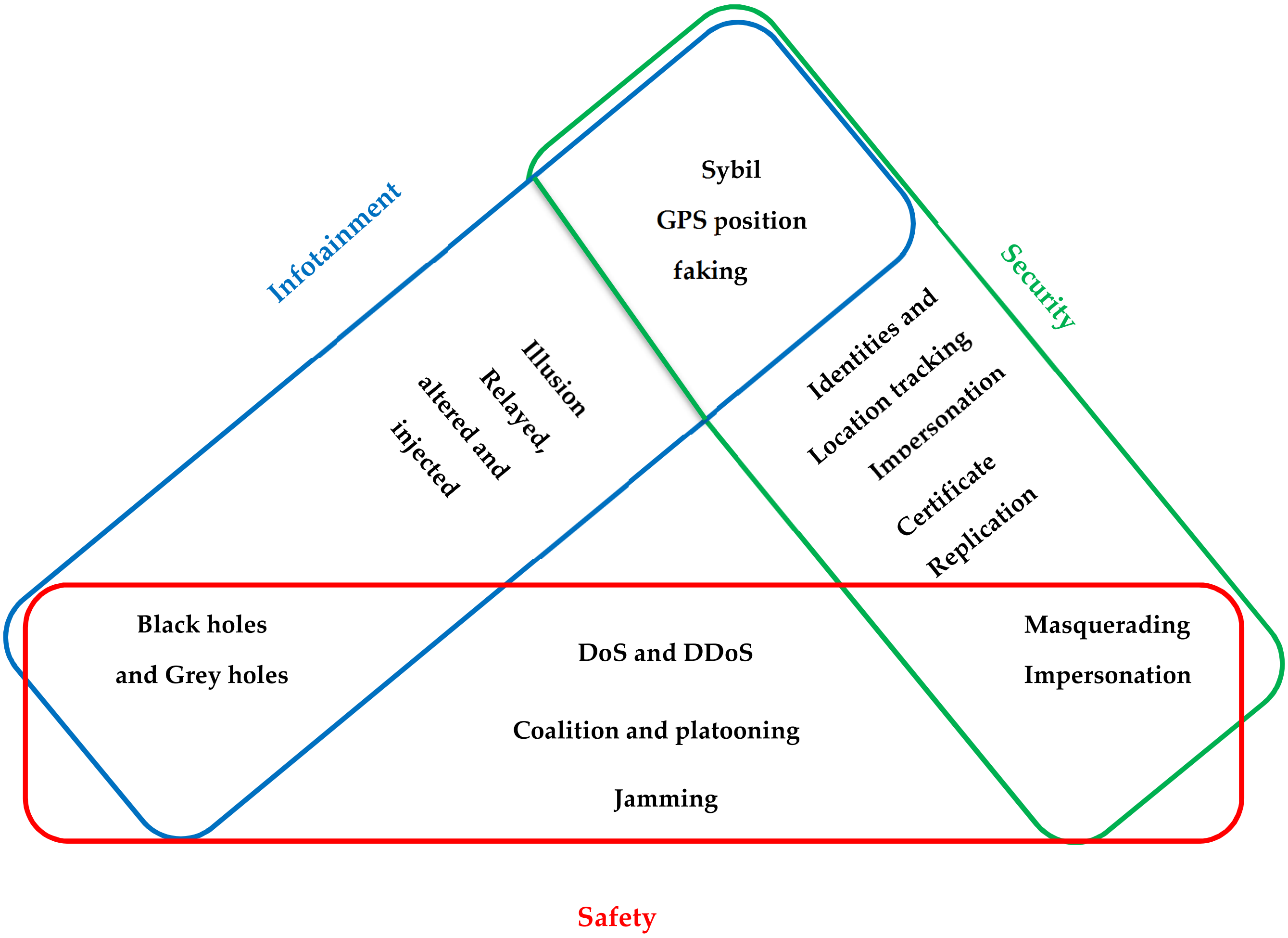


Figure 2.3 Security threats for VANET Applications [60].

2.6 Intrusion Detection System (IDS)

In autonomous and semi-autonomous vehicles, two security layers are proposed to protect external and internal communication systems of these vehicles: Intrusion Prevention System (IPS) and IDS [71]. The IPS is the first layer security system and IDS is the second layer security system of a network or computer host [81]. Security measures have become a hot topic in automotive systems as the first security layer did not have the ability to provide sufficient security [82]. In addition, the external communication of these vehicles can offer a variety of services such as safety applications and non-safety applications, which supports increasing research efforts and growing interest in security systems.

IDS is considered as one of the most effective means of protecting VANETs as these mechanisms can identify abnormal or malicious activity on the network or the host [22]. IDS has the ability to achieve sufficient security and privacy of systems or networks because it plays an important role in detecting and blocking internal attacks that cannot be detected or prevented by other security approaches.

The high dynamics of a topological node for VANETs can be difficult to apply using IDS of self-driving vehicles [83] because the security system cannot obtain enough data (features) from the mobile nodes to build a comprehensive view of the network. To overcome this problem, some novel features are extracted from self-driving vehicles, such as ICMetrics features from automotive sensors, to achieve authentication and detection.

2.6.1 IDS Classification

IDS can be categorised in various ways, but an often used classification is: 1) anomaly, 2) misuse and 3) specification based detection systems. Each detection methodology has features that distinguish it from others, whether positive or negative, but all these approaches try to provide sufficient security, as well as prevent and detect all unauthorised access from malicious vehicles or nodes [84].

1. A signature-based system: in this detection technique, the security system contains a database of the typical behaviour identified for known attacks. The data set is compared to the behaviour of the system, and when there is a match this shows that there is an intrusion.

2. An anomaly-based system: this type of detection depends on the behaviour that had been previously determined. If there is any deviation from this behaviour, there is an intrusion. Essentially, the detection system is based on a profile created from the normal behaviour of the network.
3. A specification-based system: this detection system defines a set of conditions that must be available in the protocol or program. The intruder is detected in the event that the system does not meet these conditions.

2.6.2 Architecture of Intrusion Detection System

There are other classifications of intrusion detection systems depending on the architecture [85]: 1) stand-alone, 2) distributed, 3) hierarchical and 4) mobile agent.

1. **Stand-alone IDS**: each vehicle is relying on local resources for data collection, so it does not exchange data. In this scenario, the vehicle has no information about the position of other vehicles.
2. **Cooperative and distributed-IDS**: this mechanism relies on cooperation between vehicles and RSUs to detect intrusion. The very nature of self-driving requires the exchange of information between vehicles or with the infrastructure. This cooperation can detect penetration through the information which is exchanged between the vehicles. The main problem with this type of detection is that it may affect the performance of the network.
3. **Hierarchical IDS**: this approach is based on the detection of a division of the network into groups (clustering); each set contains a head and there is cooperation between these nodes. This method of detection may reduce the burden on the network. However, the problem is that there needs to be a comprehensive view for the network due to the lack of cooperation between

the vehicles on the network. Some types of attacks may not be detected; for example, distributed attacks.

4. **Mobile Agent for Intrusion Detection:** this approach uses mobile agents to perform a specific task on a node. This architecture allows the distribution of tasks in intrusion detection.

There are many mechanisms that can be used in the protection of the communication system of self-driving and semi-self-driving vehicles. Conventional security mechanisms, such as cryptographic methods, cannot detect internal attacks. Thus, as indicated above, a second layer of defence is required alongside encryption to increase the security of the networks or systems.

2.7 Simulation for VANETs

The evaluation process of current trust prototypes for the external communication systems in autonomous systems is mostly done via simulation systems [60]. Many researchers have shown the important role of simulation systems. According to Shannon: "the process of designing a model of a real system and conducting experiments with this model for the purpose of understanding the behaviour of the system and/or evaluating various strategies for the operation of the system" [86]. Simulation systems are considered very important in VANETs. In this case, any protocol or a new protection method has to be applied in simulation due to the fact that these projects incur significant costs.

There are many simulation systems that are used in the field of vvehicular ad hoc networks. Figure 2.4 shows the classification of simulation software for networks of vehicles. Simulation programs in VANETs are divided into three categories. They are [87]:

1. Vehicular mobility generators.
2. Network simulators.

3. VANET simulators.

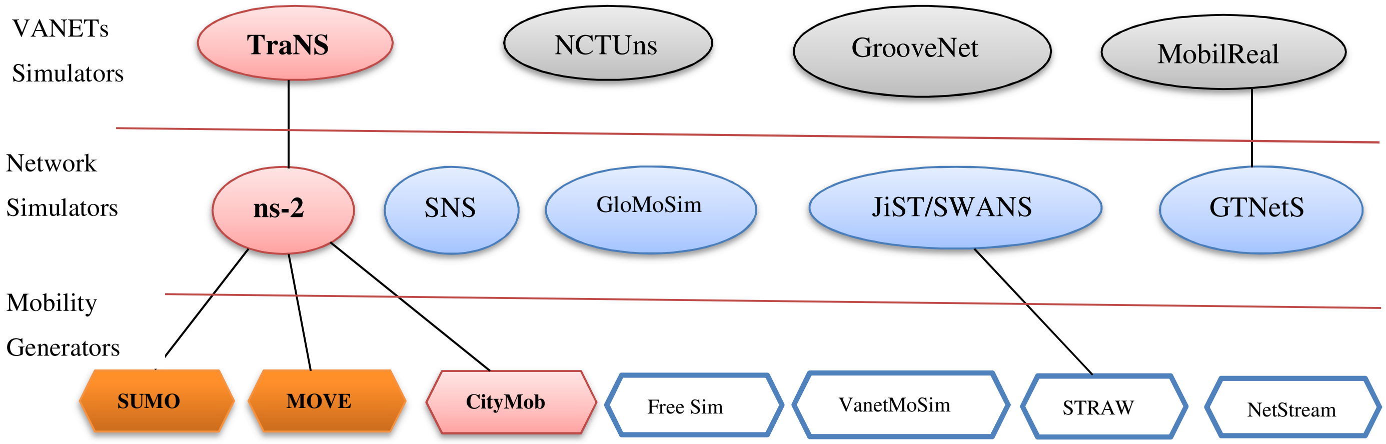


Figure 2.4 A Taxonomy of VANET Simulation Software.

Vehicular network scenarios used in this research are closely linked to real-life traffic mobility conditions. Most simulation systems are designed for MANETs; when these programs are used for simulating the VANETs, the proposed system needs extra programs (such as using the vehicular mobility generators).

The ns-2 is a simulation system with open code, designed to work on the Linux operating system and may be run under Windows operating system with Cygwin [88]. This system simulation has proved a lot of studies and experiments efficiently for various protocols of the networks. In 1989, researchers began considering ns-2 as an alternative system to a real network [89]. To study the real behaviour of VANETs and without any effects of unknown or desirable than other protocols, using the Constant Bit Rate (CBR) traffic generator with protocol UDP; this is very close to the real behaviour of the network.

In ns-2, two types of languages are employed to increase the efficiency of the simulation (Tool Command Language (TCL) and C++). The TCL script file is used to specifying the path of movement nodes and communication behaviour, as well as a path of trace files (the output of simulation takes two files which are traced and Network Animator (NAM) file). Figure 2.5 illustrates the input and output files for the ns-2.

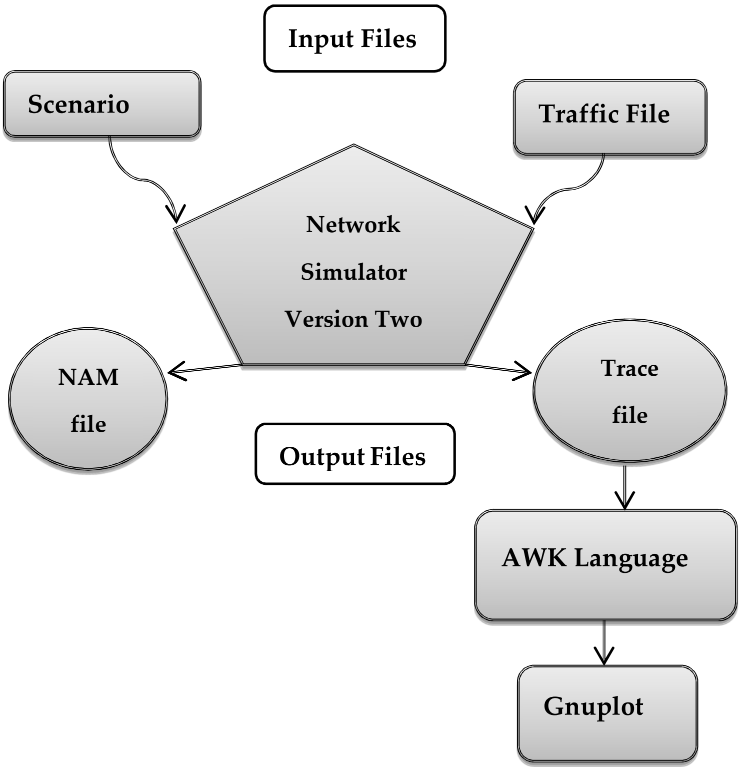


Figure 2.5 Input and Output Files for ns-2.

2.7.1 Tool Command Language (TCL) Simulation Scripts

This language was created by John Oosterhout [90]. The properties of this language are:

1. It allows fast development of the projects for programmers or developers.
2. It is easy to use compared with other languages.
3. It is flexible and free.
4. It provides a graphical interface Network Animator (NAM).

The output of the ns-2 simulator has two files which are NAM and trace files. TCL language determines a number of important issues in the software simulation, including:

- Physical and protocol type specifications.
- Creation and movement of nodes (scenario file).
- Node communication (traffic file).
- Event logs such as trace file and visualisation setup such as NAM file.

In the TCL file, there are a lot of parameters that must be defined, such as radio propagation models (Free space, Two-Ray Ground reflection and shadowing). The Two Ray Ground is utilised in this research. For studying the behaviour of the protocol, simulation system can store a file tracking and then we can use an analytical language. Many types of files tracking are available in the ns-2 simulator, such as agent, route and MAC trace. Simulation system contains some practical limitations, such as the number of nodes or processor speed [88].

Through the course of this thesis, the design security system with response system are employed by ns-2 [88]. The ns-2 component-based C++ and OTCL simulation library and framework primarily for designing network simulators. There are other commercial network simulators such as OPNET [91], EstiNet [92] and QualNet [93], and free ones such as GloMoSim [94], ns-2 [88] and JiST/SWANS [95].

2.7.2 Why Do We Use Network Simulator Version Two (ns-2)?

Network Simulator version two, commonly known as ns-2, is one of the most important and most widely used simulation systems in the world [96]. The ns-2 has some properties that encourage researchers to employ it in their works, such as open source, efficient, a rich library and common application in scientific research area [97]. In addition, most of the proposed systems have utilised the ns-2 network simulator as shown in Figure 2.6 [60], [98].

2.7 Simulation for VANETs

For a proposed security system is on physical, Data link and Network layer the researchers prefer to employ ns-2. On the other hand, if the proposed security system is for transport, application layers, then ns-3 is highly suitable [99].

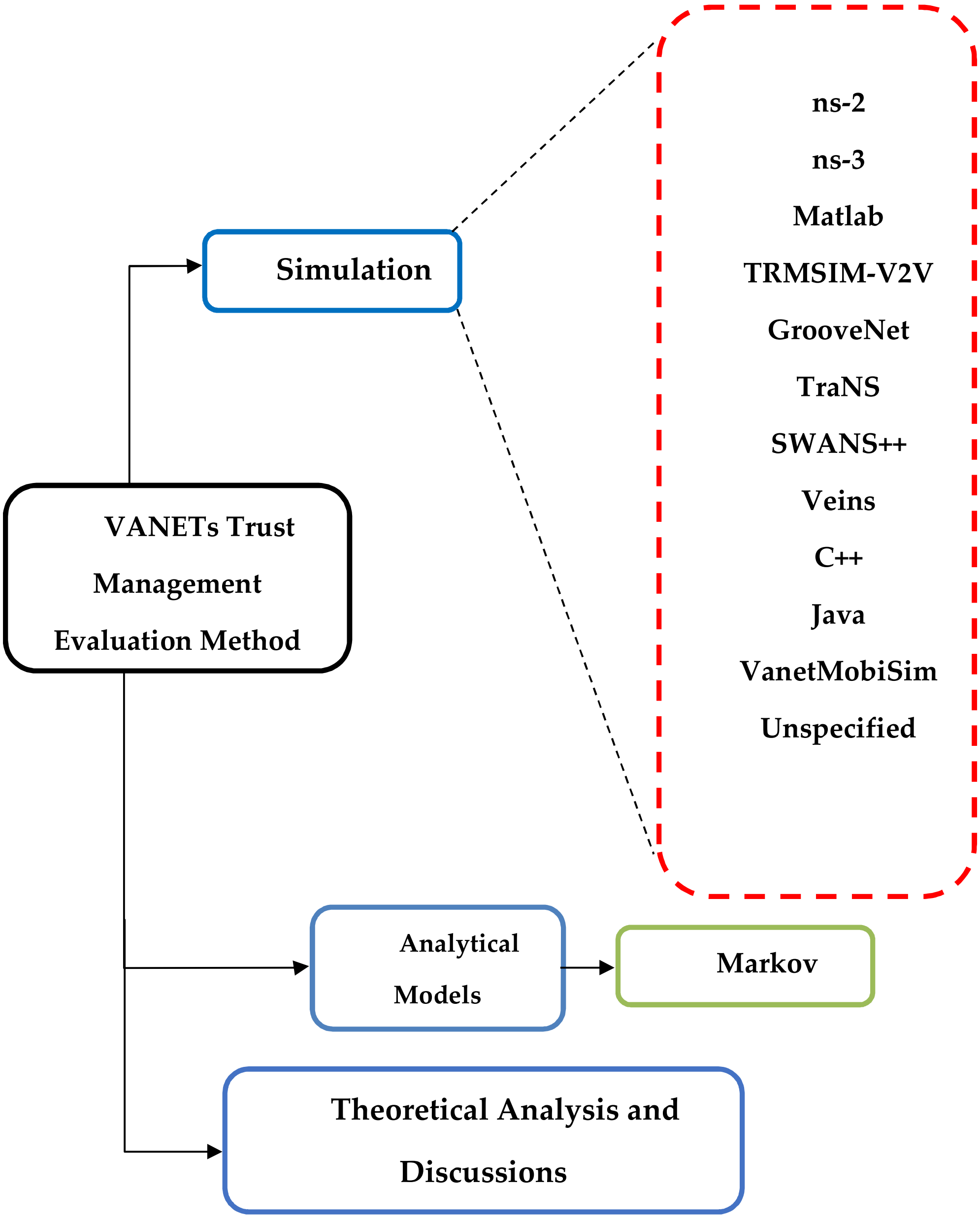


Figure 2.6 Evaluation of Trust Approaches for Vehicle Networks [60].

In Figure 2.6, the evaluation methods for the current trust models are summarised with the suitable simulators environment for VANETs [60] .

The simulation system passes through three essential stages which are [98]:

1. Step One (**Simulation Design)**: At this stage, the user must specify the purposes of the simulation, network configuration, assumptions, performance measures and type of the expected results.
2. Step Two (**Configuring and Running Simulation)**: This step consists of two phases, which are network configuration and simulation phases. The network configuration could be TCP/UDP, while in the simulation phase, we must determine the clock and execute events chronologically (threshold).
3. Step Three (**Post Simulation Processing)**: This phase involves verifying the integrity of the program and evaluating the performance of network simulation.

Specially, the simulation system in vehicular ad hoc network needs two types of files for random traffic connection, such as a traffic-scenario generator script and mobile pattern generator. These files are generated by special programs or the researcher, program generates these files. Through these programs, some parameters are set that are needed in the formation of the files. For example, the number of nodes, the maximum number of connection and seed, etc. There is no relationship between the number of vehicles and the maximum number of connections

2.7.3 Why Do We Need to Generate a Realistic Environment for VANETs?

The mobility model in VANETs is considered one of the most significant parameters when testing or evaluating any algorithms or protocols proposed due to high mobility vehicles in VANETs [100]. Generally, the mobility model is divided into two types which are urban mobility model and highway mobility model [101]. Most existing researches are concerned with city mobility model [102]. The urban mobility model has many features that distinguish it from other mobility models, such as:

- Low speed.

- Heavy vehicle density (traffic).
- A lot of crossings along roads

At present, urban mobility models utlise many types of modes or models, such as the Random Way Point (RWM) model, Manhattan mobility mode, Rice University Model (RUM), Stop Sign (SSM), Probabilistic Traffic Sign (PTSM) and Traffic Light model (TLM) [101]:

1. The Random Way Point Model (RWM): The vehicles are initially distributed randomly or uniformly distributed for the VANETs. This model is the most widely used for VANETs simulation [103].
2. Manhattan mobility mode [104]: This model uses the grid road topology. The vehicles can move in a horizontal or vertical direction. The probability of the vehicles to turn left or right is 0.25, while the probability to go straight is 0.5.
3. The Stop Sign Model (SSM) [105]: This model is urban mobility model that uses stop signs as the traffic control mechanism for vehicles.
4. The Probabilistic Traffic sign Model (PTSM) [105]: This model is an improved version of the previous model (SSM). It uses the red signal to stop the vehicles and green signal to allow vehicles to pass.
5. The Probabilistic Traffic Sign (PTSM): In this model, the vehicles intersection with the empty queue, stop at the signal. It improves the previous model SSM.
6. The Traffic Light Model [105]: The researchers considered it the most realistic model in comparison with the other models. This model has more flexibility moving the vehicles than the other.

In the Highway Mobility Model (HMM), the vehicles have attributes, such as high speed, no traffic lights and a few number of RSU. These attributes distinguish the HMM from the urban mobility model [101]. The current research, the HMM is not fully explored in experimental research [102] ,[106]. Girinath is considered one of the researchers of VANETs is to employ HMM for the vehicles rather than the urban mobility model.

Vehicular traffic is possible to describe the two are microscopic and macroscopic approaches [107]. Macroscopic: refers to the density of traffic (number of vehicles per kilometre of the lane), while the microscopic is to determine the movement of every vehicle alone.

2.8 Intrusion Detection Systems - Survey

The life-saving decisions in self-driving vehicles are heavily based on received information from other vehicles/RSUs in that radio coverage area. Vehicular communication can make driving safer, more efficient and more comfortable. Hence, security systems are considered a very important requirement in VANETs for many years [108]. In addition, numerous research papers and many experiments have been conducted on vehicular ad hoc networks because of their importance to many applications in self-driving and semi-autonomous vehicles.

To achieve security characteristics in VANETs, researchers have proposed some security techniques, such as cryptography and digital signatures. These security mechanisms play an important role in ensuring nonrepudiation and integrity of CAMs, warning messages, notification and control data which are exchanged between vehicles and RSUs in that zone. In [109], [110], [111] digital signature schemes have been proposed for VANETs. The public key infrastructure has been designed in various security systems to protect VANETs from potential attacks [50], [112], [113]. Despite all the proposed intrusion prevention techniques, internal attacks can transmit false information to other vehicles/RSUs in that radio coverage area. In other words, insider/internal attacker is able to launch its malicious behaviour even in the case of strong traditional security systems, such as cryptography and digital signature schemes [108].

2.8 Intrusion Detection Systems - Survey

The most reliable security system to protect the external communication system in autonomous vehicles is intrusion detection system [114]. IDS has the ability to identify internal and external attacks with high performance detection rate [114]. In addition, IDS is effectively able to detect inside and outside attacks at real time. However, to work properly, it needs strong identification and authentication system [108]. Hence, a novel authentication system is designed in this thesis to support detection process of IDS. Furthermore, artificial intelligence techniques are utilised in building IDS to predict new attacks from unknown attacks in this thesis. In the following section, we explain some of the related work.

2.8.1 Anomaly and Signature Intrusion Detection Systems

A research on threshold determination for processing spoofed data in VANETs is carried out to find the best possible threshold in [115]. The authors show that this threshold plays an important role as decisions and steps are taken based on reaching the defined threshold. If the threshold is kept high, there is an evident delay in decision making on part of the vehicles. The research studies the threshold as a Kalman filter which can be updated dynamically. The proposed work suffers from bootstrapping but is effective in reducing the percentage of wrong decisions.

Adversaries can attack a VANET in many different ways. One method of attacking a vehicle is by inserting ghost vehicles in the network. Doing so creates nodes that do not physically exist but can impact the functioning and safety of other vehicles in the same zone. In [116], the authors propose a central detection scheme which uses trust and misused information from misused reports to determine and eliminate adversaries from a network. Simulations of the proposed scheme show that an adversary can be obfuscated if three spoofed nodes are placed on the network. The authors also show that cooperating adversaries can be eliminated if only 37% of neighbouring nodes collaborate with each other.

Zhang et al. are considered the first researchers to propose the use of IDSs in ad hoc networks [117]. A cooperative distributed- IDS is proposed to detect malicious activities in ad hoc networks. Two detection engines are proposed which are: local and global. IDS agents are designed for each node in network for collect data and detect processes of abnormal behaviours in local detection engine. Furthermore, neighbour's nodes can exchange/cooperate important information with each other in that radio coverage area to form a cooperative detection engine. These detection techniques have the ability to prevent some attacks of DoS on ad hoc networks.

Zaidi et al. proposed an intrusion detection system for VANETs. The proposed security system is evaluated under normal and abnormal conditions to check its efficient detection of rogue nodes [108]. Statistical techniques are employed in the proposed IDS to identify false information attacks. The authors can approve that application-layer IDS is more efficient with dynamic network or high change topology, such as VANETs. In other words, a cooperative information exchange plays an important role in enhancing detection rate of IDS.

In [118], the authors proposed a watchdog IDS that is based on Bayesian filter to detect attack vehicles and decrease the number of alarms of vehicle. Watchdog mechanism monitors vehicles behaviour and selects the safest path between sources to destination through Pathrater. This system can identify malicious vehicles which drop received packet rather than forwarding them to the destination node. It is mainly based on communication information that was collected from neighbour's vehicle. On one hand, the main advantage of this security system is that is detects misbehaving vehicle in many cases. On the other hand, watchdog IDS cannot detect malicious vehicles in cases of partial collision and collusion. Sometimes, watchdog method detects some vehicles as malicious nodes, but in fact they are normal nodes. In this case, Bayesian filter is utilised to check whether the identified vehicles are attackers or not.

Chaudhary et al. in [119] proposed an anomaly intrusion detection based on fuzzy logic to protect MANETs from potential attacks. It can detect packet dropping attacks as well as isolated malicious nodes based on their internet protocol (IP). In addition, the fuzzy intrusion detection system has the ability to save the power resources by removing the suspicious nodes in MANETs. It is noticed from the simulation results that it can detect the malicious nodes with low false positive alarm and high rate of true positive alarm in MANETs.

Zhou et al. designed a security protocol to protect the VANETs from Sybil attacks [120]. The authors have explained the use of encryption technologies to reduce the number of attacks on VANETs. It is a lightweight, efficient and scalable protocol that has the ability to provide sufficient safety environment for VANETs against malicious activities. In these scenarios, each vehicle would contain a number of pseudonyms used during their communication. The malicious vehicle in this protocol is pretends/ broadcasts multiple fake IDs to confuse other vehicles in that radio coverage area. The detection process of the proposed security system does not require any vehicle in VANETs to disclose its identity. The authors can enhance the Department of Motor Vehicle workload to road-side boxes to provide a security system with low information overhead. It is noticed from the simulation results that the security system can detect Sybil attacks in VANETs with a low delay, communication overhead with a high accuracy of detection. However, these techniques carry large constraints, such as computational complexity.

Li et al. have designed a trust management approach to create safety and security environment for VANETs [121]. The detection system is proposed in this paper to secure vehicle network that was based on an attack-resistant trust management scheme (ART). It has the ability to detect and adopt with abnormal behaviour in VANETs. In addition, the trustworthiness of both mobile node and data are evaluated in this security method. Practically, the data collected from multiple vehicles with sensors are used in assessing data trust of the proposed system. In other words, two dimensions are utilised in evaluating the trusted vehicles which are: recommendation trust and functional trust. Extensive experiments are employed to validate the effectiveness and efficiency of the ART approach. The ART is applicable to a wide range of applications in VANETs to enhance traffic safety, mobility, and environmental protection.

In [122], the adaptive detection threshold is utilised in designing security system to detect intelligent malicious behaviours in VANETs. It can detect immediately any abnormal behaviours in vehicle network are generated from mobile vehicles. However, the proposed system can detect malicious activities with high rate of packet delivery and detection process.

A security system is designed to secure VANETs from fake vehicles that is based on innovative signature based intrusion detection system [123]. Applying a plausibility model verify vehicle movement information. Moreover, it can detect fake information whether fake traffic congestions from RSUs or fake information from attackers. In this case, attackers try to insert moving vehicles data into the VANETs to deny the real congestions.

Coussement et al. have proposed using an intrusion detection system to detect malicious activities that have direct and negative impact on the performance of external communication system in vehicles [83]. It analyses incoming and outgoing traffic packets to distinguish attack actions. The detection process of IDS is based on decision making mechanism to protect sensitive information from potential attacks in VANETs. More specifically, two schemes of IDS are installed in the first one on vehicles whereas the second one on RSUs. These IDSs work together to create groups of vehicles based on their speed. However, the main work the proposed IDS depends on two IDS approaches and clustering of vehicles. When an intruder launches its attacks, the security system broadcasts warning messages and alerts neighbouring clusters.

2.8.2 Intrusion Detection for Routing Protocol

A new Position Based Secure Routing Protocol (PBSRP) is presented in [124]. To secure routing protocol in VANETs from malicious drivers, the PBSRP integrates Most Forward within Radius (MFR) and Border based Most Forward within Radius (B-MFR). Station to station key agreement protocol is utilised to add to the security system in this protocol to protect the VANETs from different attacks. Therefore, the proposed security system consists of three phases which are: initialisation, optimal node selection and secure data delivery. In terms of PDR and end-to-end delay, it is noticed from the simulation results that the performance of PBSRP is better than MFR and B-MFR when attacks are included in the VANETs.

In [125], a security system is proposed to minimise one of the DoS attacks which is grey hole attacks. In this approach, the authors assume that each communication node is utilising only the internal knowledge which is gained by routing protocol. The system is based on the internal information of routing protocol that is employed in network layer of network. Various threats are used in evaluating the performance of the proposed security system. It is noticed from the simulation results that the security system can reduce the number of drop packets by 51%. Hence, it plays a vital role in creating stand-alone safety system in ad hoc network from grey hole attacks.

A cooperative intrusion detection system is proposed to secure vehicle network from black hole attacks. It is based on cross layer architecture that can correlates both network and MAC layers detection [126]. The security system in this paper is proposed to enhance the watchdog model based routing level monitoring. The detection process of the cooperative intrusion detection consists of two phases which are: 1) monitoring the number of requests to send/clear the watchdogs and identified vehicles at the MAC layer; 2) recalculating watchdog's detection percentage. In this security system, the presence of channel collision is recognised by cooperative monitoring in both layers that help to reduce the number of false alarms. The experimental results corroborate that the cooperative detection can enhance the detection rate and reduce the number of false alarms.

Guo et al. have designed privacy protection to secure vehicles communication systems for VANETs [127]. The proposed protection mechanism is able to combine digital signature mechanism, symmetric encryption, homomorphic key agreement and message authentication to provide adequate protection for communication protocol. Hence, the combining process in this paper can prevent personal information of users form any illegal access. This proposal can enhance the security and privacy of the transmission messages that are exchanged between vehicles and RSUs. It also has the ability to reduce computation costs of privacy and security in VANETs.

In [128], the authors proposed a new security system to protect routing protocol in VANETs. An anomaly detection system can detect and prevent wormhole and rushing attacks that have direct and negative impact on the performance of routing protocol in the external communication systems in vehicles. A statistical approach is utilised in designing intrusion detection that monitors vehicle's path selection. However, it can detect and prevent any malicious behaviours from VANETs. It is noticed from simulation results that the proposed security system exhibits high accuracy of detection rate.

Usha et al. proposed a protection mechanism of the AODV routing protocol in ad hoc networks [129]. It can provide an authentication aspect for each node in network through route discovery that detects and isolates one of the DoS attacks which is black hole attacks. This security proposal plays an important role in increasing the rate of PDR and throughput for network. In addition, in single round time of path established between source to destination, the security system can prevent black hole attacks with low computation overhead on network.

2.8.3 Intrusion Prevention Systems

Cryptographic schemes are often based on the use of public private key pairs for the provision of security. These keys are often updated according to the instructions from a certification authority. When a vehicle has limited connectivity, it may not be able to update the key pairs. A solution to this is that often used multiple key pairs are stored on the vehicle. The need for secure storage can become a security concern. In [130], the authors showed that it is possible to entirely eliminate the need for stored keys by using Physically Unclonable Functions (PUF). The authors study a vehicle's on-board unit as the basis of a PUF to create a secure storage for vehicle.

In [131], the authors stated that cryptographic systems can be used to secure VANETs. As they are insiders in a VANET, therefore the cryptographic key used can be captured which could lead to the system being exposed. The authors showed that it is possible to detect malicious insiders with a high precision by simply studying the disseminated redundant information. The authors have proposed three graph-based metrics which they apply to the geocast protocol and the aggregation protocol. The authors have reported mixed simulation results as the geocast protocol does not effectively detect redundant data, whereas the aggregation protocol can sufficiently detect conflicting data.

Security in VANETs can be attained through the use of cryptography. The use of resource hungry cryptographic algorithms can have a negative effect on resource constrained networks like VANETs. The authors in [132] studied the design of a cryptography based system for VANETs. The proposed system uses a single cryptographic key with AES encryption. The authors also tested the proposed system with public key cryptography and RSA encryption. The research shows that RSA outperforms AES when simulated in VANET composed of 15 mobile nodes under AODV routing.

In a recent research [133], the authors discussed that even in the presence of encryption-decryption, vehicular ad hoc networks remain insecure. The research shows that cryptography can prevent external attacks but internal attacks cannot be prevented. The authors show that the prevention of internal attacks can be achieved through misbehaviour detection mechanisms. The authors have implemented a malware application on a physical vehicle and showed that this can be used to prevent internal attacks which are prevalent due to the lack of security standardisation in VANETs.

Research [134] on security in VANETS has shown that the network has security implications on the security of the drivers and passengers. Cryptographic services come at a cost, like computation time and power, which is why resource-efficient methods are often required. The authors claim that the security of a vehicle is incomplete without the awareness of surroundings. Previously, the Awareness Quality has been used in networks to study the effect of network congestion. The authors have used the awareness quality to study the positive and negative effects of omitting security certificates in VANETs. The authors have simulated their work through the use of various metrics and indicators.

In [135], the authors proposed a security scheme for wearable devices using the ICMetrics security. The authors demonstrated how ICMetrics can be generated using the MEMS accelerometer and other sensor characteristics. The authors designed a comprehensive security scheme that generates ICMetrics for a device. The ICMetrics are then used to generate a symmetric key, which is used for the provision of security services like authentication, integrity, and confidentiality. The authors have simulated their scheme and concluded that higher levels of security can be provided without a compromising the resource (memory, time and speed) requirements.

In [136], the authors did a comparative survey on the complicated issues of pseudonymity in VANETs. They have determined four major classes of pseudonym approaches that are most commonly used to secure the external communication of vehicles. Pseudonym approaches are covered in this survey that are based on identity-based cryptography, public key, symmetric authentication and group signatures. The authors discussed relations between each class of pseudonym and its life cycle. The various schemes are compared to identify the research challenges and standardisation issue in the state-of-art.

Zaidi et al. in [137] discussed various issues in security and privacy of vehicular internet which have a vital role in bridging all the security holes. The authors emphasise the important role of security and privacy in vehicular communication system. In other words, the reliability, privacy and integrity are ensured for road conditions information, control data, CAMs and warning messages in the external communication system of vehicles. They have proposed some suggested solutions for internet security breaches in VANETs. These security solutions are proposed to provide protection and privacy for vehicular applications. One of the solutions, is digital identity approach which is proposed for vehicular communication. i.e., liable for the vehicle held by driver rather than another vehicle. In addition, a new digital identity is formed from Vehicle

Identification (VID) and driver (DrL). In other words, the driver license authority and vehicle registration are merged into one identity.

In [138], verifiable multilateration is proposed to protect position verification for vehicles. The work is based on information of base stations/RSUs. i.e., it is working even if vehicles which do not have GPS for positioning. In other words, the RSUs in this approach are considered as a trustworthy party to determine the vehicles position. The collaboration mode is utilised from four RSUs to determine the vehicle position by calculating the time between sending and receiving. i.e., the total time between inquire and answer.

Leinmüller et al. explained the security issue for critical applications of the communication systems in vehicles [69]. They presented an overview of the concepts that improve the security schemes of communication between vehicles and they assessed the security requirements. The concept of security is categorised into two classes based on the type of primitive work: proactive and reactive. The authors have concluded that some security solution does not fit into the design constraints of external communication system in vehicles. Hence, the less protected schemes will possibly have to adequate.

In [139], a security protocol is designed to provide location privacy in VANETs. It can prevent Sybil attack from illegally access VANETs. The short group signature approach and batch verification are employed in designing security systems. It is noticed from the simulation results that the detection system is efficient and effective in securing vehicle to vehicle communications. In this paper, the authors proved that the proposed Sybil detection system is more efficient when compared to rivalling approaches, such as Footprint and Privacy-Preserving Detection of Abuses of Pseudonyms (P2DAP).

Nema et al. proposed an encryption and decryption schemes to protect traffic system for vehicles communication [132]. The encryption system is based on

Rivest-Shamir-Adleman Cryptosystem (RSA) algorithm and Advanced Encryption Standard (AES) key-management to protecting sensitive information and controlling data between vehicles from malicious vehicles. MATLAB was utilised for the proposed security system. It can identify and remove vehicles with misbehaving from network. Furthermore, it can provide integrity and confidentiality of the control data, warning messages, CAMs and notification messages in VANETs.

Zhang et al. proposed a new privacy-preserving system to secure VANETs from malicious activities [140]. The authentication security protocol is designed to overcome common problems in existing privacy-preserving communication protocols in VANETs, such as fast and not based on tamper-proof devices (TPDs). The idea of the proposed security system depends on the distributed aggregate privacy-preserving authentication for VANETs. In other words, a new multiple trusted authority is utilised in designing the authentication system. The security system in vehicles can confirm many control data messages, CAMs and notification messages simultaneously that are based on aggregate signature technique. The authentication system plays an important role in reducing the storage space by the compressing the verification process of messages with their signatures into a single one. This security system only needs realistic TPDs that makes it more practical.

2.9 Routing Protocol for Vehicular Ad hoc Networks

Routing protocols in VANETs play a vital role in transmit/receive control data and sensitive information between vehicles and RSUs in that radio coverage area. Example of information that was exchanged are CAMs, notification messages and warning messages. The routing protocol in the external communication system of autonomous vehicles are classified into two types which are: routing information and transmission schemes [141]. In addition, routing information is categorised into two types: topology-based and geographic-based routing. Whereas, transmission schemes are divided into unicast, multicast and broadcast.

In order to transmit data/information to all vehicles, the self-driving vehicles need a routing protocol that handles messages and avoids collisions and congestion. Choosing the appropriate routing protocol is one of the most important things in the external communication systems in autonomous vehicles.

The source of information of topology routing protocol is link's information that is stored in routing tables of vehicles [142]. Routing information source for vehicles that are based on position routing protocols is GPS. Geographic-based routing protocol is widely used in the external communication for semi-autonomous vehicles. Greedy Perimeter Stateless Routing (GPSR) is one of the geographic routing protocols that is utilised in VANETs [143].

The principal work of GPSR is based on GPS information to achieve transfer/receive information between vehicles and RSUs. Unfortunately, inaccurate position information of GPS is considered a major problem in determining the vehicles localisation [144]. In other words, the error rate of GPS in determining a vehicle position may reach 20 metres which is unacceptable in self-driving vehicles [144]. In addition, the position systems of vehicles that rely on GPS are unable to work under in tunnels. All these reasons have encouraged researchers to remove GPS from driverless vehicles and find alternative techniques, such as e-maps [145].

In this case, the routing protocol that is based on GPS information has become impractical in self-driving and semi-autonomous vehicles. Thus, routing protocols in vehicles which rely on the link's information are more efficient than protocols based on topology information. Selection process of routing protocol depends on the nature of the network [146]. Figure 2.6 below shows the types of protocol used:

2.9 Routing Protocol for Vehicular Ad hoc Networks

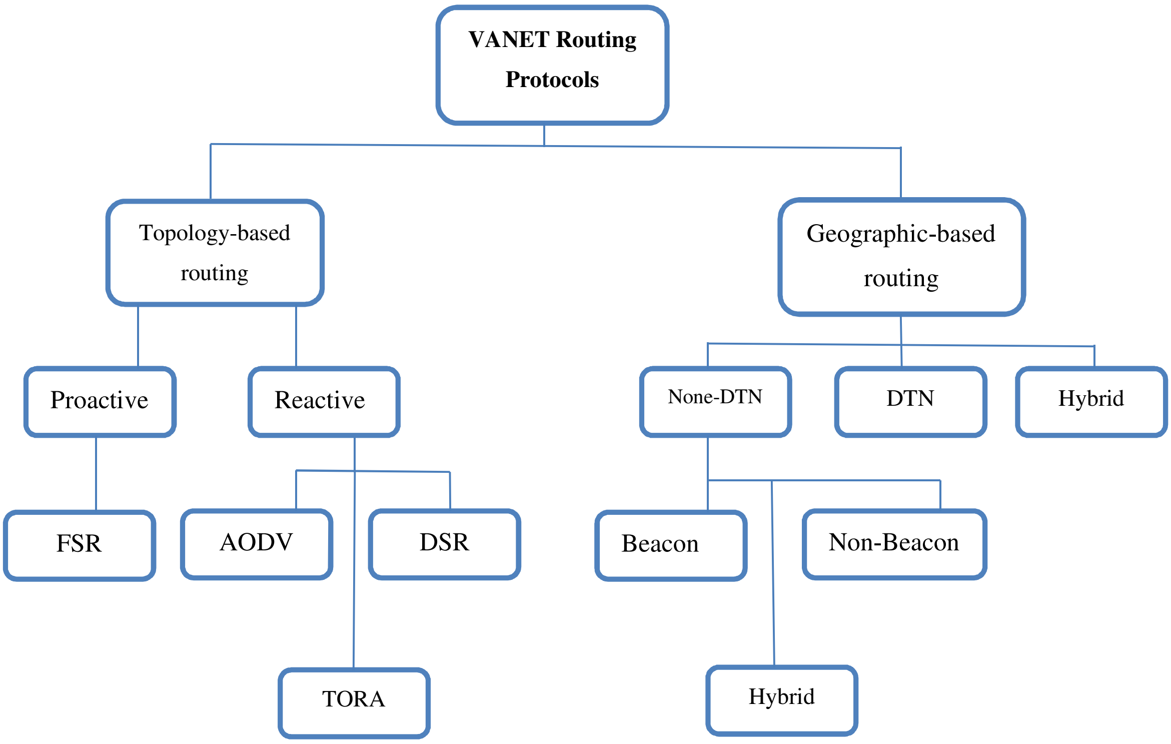


Figure 2.7 The Types of Routing Protocols in VANETs.

In this thesis, the topology-based routing protocol is utilised in designing a communication system in autonomous vehicles. This protocol is divided into two types proactive and reactive routing protocol [141].

- **Proactive Protocol**: routing information to send the package to the next hop must be addressed without attention to the connection request.
- **Reactive Protocol**: this type of protocol transmits packets only to the available paths. This will reduce the burden on the network.

In this research, the reactive routing protocol is utilised in designing a communication system of self-driving and semi-autonomous vehicles. It has many types such as Ad hoc On Demand Distance Vector (AODV), Dynamic Source Routing Protocol (DSR) and Temporally Ordered Routing Algorithm (TORA) [141]. These routing protocols are suitable for MANETs.

Routing protocols in MANETs cannot be applied directly to the VANETs. They need major adjustments. The routing protocol AODV is suitable for working in an environment for vehicles (VANETs) [59], and will be utilised in our research. The research reasons for choosing this protocol:

- AODV can quickly adapt to the rapid change in the network topology, because it is only maintained on one road.
- AODV is appropriate when we have a large number of vehicles.
- AODV reduces the flooding of messages in the network compared to the other protocols (reduces the burden on the network).
- This protocol can respond even if the connection fails.
- AODV utilises sequence numbers that help to certify the freshness of paths and it can avoid a loop topology.
- The performance of AODV is the closest to GPSR that was confirmed by many studies [146].

Important features of possible application of this protocol on a large-scale compared with other protocols. This feature is considered important for VANETs.

Table 2.1 shows the similarities between AODV and GPSR routing protocol. The same forwarding strategy and scenario are employed in AODV and GPSR which are Greed forwarding and scenario in urban area.

Table 2.1 Comparison between AODV and GPSR.

	AODV	**GPSR**
Forwarding Strategy	Greedy Forwarding	Greedy Forwarding
Scenario	Urban	Urban
Mobility	No	No
Road direction	Single direction	Single direction

However, these routing protocols do not provide the mobility model. In addition, single direction is considered a road direction in AODV and GPSR. It is easily observed from table 2.1 that AODV and GPSR have the same characteristics. These characteristics make AODV protocol the closest to the GPSR protocol.

2.9.1 Improved Ad hoc On Demand Distance Vector

In external communication of self-driving vehicles, a routing protocol can dynamically establish communication paths between the source vehicle to the destination vehicle. In other words, the exchanged packets between two vehicles have more than one path $(p1, p2, p3, p4, \dots\dots\dots\dots \; and \; pn)$, where n is the number of available paths.

In this thesis, one of a reactive on demand protocol is enhanced to adapt with VANET parameters which is VANET-AODV. This protocol consists of three phases which are: route discovery, data transmission and route maintenance.

a. Phase one: Route discovery in VANET-AODV

In this phase, route request (RREQ) packets are broadcast in VANETs on available routers. The proposed routing protocol has the ability to select the path that is more stable than others. In more details, the proposed protocol can measure weight for each path based on Equation 2.1. Moreover, it plays an important role in selecting the path that has less weight to reduce overhead and burden on network.

$$Route_{Weight} = W_v * \left|V_i - V_{neighbour\ of\ i}\right| + W_D * \left|D_i - D_{neighbour\ of\ i}\right| \qquad (2.1)$$

where, the source vehicle represents by vehicle $_i$, W_v - speed weight factor, V_i is the speed of vehicle $_i$, $V_{neighbour\ of\ i}$ is the speed of vehicle $_{i's}$ neighbour vehicle, W_D is the direction weight factor, D_i is the direction of node $_i$, $D_{neighbour\ of\ i}$ is the direction of node $_{i's}$ neighbour vehicle.

b. Phase two: Route selection in VANET-AODV

To transmit data packets, the proposed protocol will choose a more stable path between two nodes when the source vehicle obtains numerous paths to destination vehicle. In this protocol, total weight for stable path will be updated in routing table and attached on each route reply (RREP) for each sent packet. The total weight path is calculated based on Equation 2.2.

$$Total\ Link\ Weight = \sum_{j=2}^{M} \left(W_V * \left| V_j - V_{j-1} \right| + W_D * \left| D_j - D_{j-1} \right| \right) \qquad (2.2)$$

where, M is the number of vehicles in the route between source and destination, j is the number sequence of vehicles in the routing table, V_i is the speed of vehicle $_j$, V_{i-1} is the speed of the vehicle $_{j's}$previous vehicle in the path, D_j is the direction of vehicle $_j$, D_{j-1} is the direction of vehicle $_j$ precious vehicle in the path.

c. Phase three: Route maintenance in VANET-AODV

In this phase, the routing protocol notifies link communication failure to source vehicles when intermediate vehicles identify link failure. In this case, source vehicles will re-send the failure packets again based on available paths in the routing table. The routing protocol will need phase two when the existing backup route fails. Figure 2.7 shows the lifecycle of routing protocol in the external communication in self-driving vehicles.

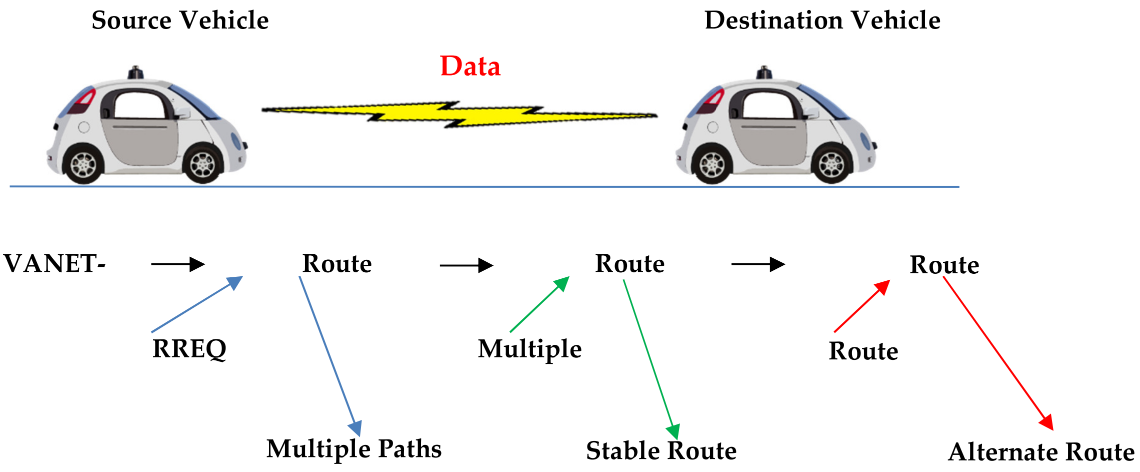


Figure 2.8 Lifecycle of Routing Protocol in VANETs.

The performance of the V-AODV protocol is evaluated by using three different metrics: control overhead, delay and PDR. These metrics are calculated under certain conditions to measure the efficiency of the routing protocol as well as comparing its performance with the original AODV. The conditions required for evaluating performance are speed of vehicles, traffic density and traffic of packets.

According to Table 2.2 and Table 2.3, the performance of the V-AODV is more efficient and suitable as compared to the original AODV in VANETs. Owing to this, the proposed IDS is applied on V-AODV to obtain a secure communication environment for autonomous vehicles. In addition, the proposed security system has the ability to adapt with existing routing protocols, such as GPSR, AODV and V-AODV.

In Table 2.2, the performance of V-AODV is compared with performance of the original AODV under various number of vehicles on roads.

Table 2.2 Performance Metrics with Density of Vehicles.

	AODV		V-AODV	
Number of Vehicle	**Control Overhead**	**Delay**	**Control Overhead**	**Delay**
50	12939	0.188s	3832	0.186s
100	13021	0.357s	3798	0.295s
150	14304	0.316s	7216	0.304s
250	18137	0.397s	11427	0.356s

According to the results in Table 2.2, we can easily notice that V-AODV can reduce burden rate on the external communication system of autonomous vehicles. In addition, the new vehicle routing protocol can reduce burden rate and time delay on vehicle communication network by up to 55% and 10% respectively. The V-AODV performance is evaluated under different vehicles speed rate as shown in Table 2.3.

Table 2.3 Performance Metrics with Speed of Vehicles.

	AODV		V-AODV	
Vehicle Speed	**PDR**	**Delay**	**PDR**	**Delay**
15k/h	**87.675%**	**0.215s**	**90.480%**	**0.078s**
25k/h	**92.068%**	**0.439s**	**92.135%**	**0.405s**
30k/h	**85.025%**	**0.358s**	**87.471%**	**0.261s**

The V-AODV performance in Table 2.3 can improve rate of packet delivery between vehicles by up to 6%. In addition, the time delay of V-AODV is up to 30% less than the original protocol. Thus, density and speed of vehicles have direct impact on effectiveness and efficiency of the routing protocol.

2.10 Summary

In this chapter, the background of the communication systems of self-driving and semi self-driving vehicles was presented alongside an in-depth study of the related works in the field of autonomous vehicles. A detailed study was presented to show that network based attacks can compromise the security of autonomous vehicles.

The literature survey evidences that security and privacy concerns in VANETs are an important area of scientific research. Several recent intrusion detection approaches were surveyed and it is concluded that existing IDS techniques are based on anomaly detection and distribution architecture. In addition, IDS integrated with mobile agents are generally more efficient in detection as compared to traditional IDS. The hybrid IDS proposed in this thesis can offer more reliability in terms of identification of suspicious/malicious activities in the external communication systems of vehicles and also enhance the accuracy of detection rate under the malicious vehicles as will be illustrated in chapters 3, 4, 5, and 6 below.

This chapter also introduces a new routing protocol that relies on link information to adapt with vehicles characteristics. It is more efficient than protocol based on topology data. The experiments show that the proposed V-AODV is more capable of adapting with VANETs with a high packet delivery rate and low end-to-end delay.

CHAPTER THREE

INTRUSION DETECTION SYSTEMS FOR AUTONOMOUS VEHICLES

"Everything should be as simple as possible, but not simpler"

Albert Einstein

Self-driving vehicles have been one of the fundamental applications within the field of modern technology [147]. These vehicles rely heavily on their communication systems, whether internal or external, to achieve their automated travel from one point to another without human intervention. Vehicular ad hoc networks are considered external communication systems for self-driving and semi-autonomous vehicles. On one hand, the application of VANETs in autonomous and semi-autonomous vehicles ensures the success of this new generation of technology based on the security of the networks. However, certain characteristics of VANETs have resulted in vulnerability at all the communication layers [20]. On the other hand, the external communication system has some properties that cause inherent security obstacles, such as speed of the vehicle, mobility, high dynamic topology, absence of a fixed security system, open medium wireless communication and density of vehicles on roads [20].

Artificial intelligence has many important applications in this scientific research area. An Artificial Neural Network (ANN) and Support Vector Machine (SVM) are employed to improve the detection rate and reduce the false alarm rate of the proposed security system. The ANN and SVM need to be trained about the normal behaviour of vehicles and this will enable it to detect malicious vehicles. Normal behaviour is considered to be an important issue in the training phase of the network.

The normal and abnormal behaviours are obtained through the trace file which describes all the events on the VANETs. The trace file is generated from the ns-2 as auditable data to detect the malicious behaviour. In other words, it contains important features that describe the normal and abnormal behaviours on roads through moving from source vehicle/RSU to destination vehicle/RSU. The proposed security system is tested/evaluated with another dataset which is Kyoto dataset to measure the performance efficiency in detecting abnormal behaviour.

In this chapter, an intelligent hybrid intrusion detection system (IDS) is designed for the external communication system of self-driving vehicles. In the dataset generation phase, a Proportional Overlapping Scores (POS) method is utilised to extract significant features from the ns-2 trace file of VANET behaviour and utilised for a classification system [148]. POS is a machine learning method that does not require any specific assumptions to be met by the underlying data. This allows POS to work on a wide range of data sets from. In addition to high predictive performance based on features selected by POS, this method has also been investigated for its stability by using the technique proposed by Lausser et al [148] in comparison to other state-of-the-art-methods. Another reason for using POS is its computational efficiency in terms of run time. In addition, the POS approach is often suitable even when the data has many classification problems, such as high-dimensional binary and outliers [149].

Reducing the number of features has direct and positive impact on computation time and memory space. These are relevant features that reflect the normal and malicious behaviours of mobility vehicles. In addition, the extracted significant features are fuzzified to overcome classification problems such as overlapping records and miss clear boarder between normal and abnormal connections. This technique plays an important role in reducing the error rate, false alarms and enhancing the accuracy of detection rate.

The hybrid intelligent IDS in this chapter is based on ANNs and SVM to detect black hole, grey hole and rushing and DoS attacks. Our research seeks to make two essential contributions:

- Designing intelligent hybrid IDSs based on the normal/abnormal behaviour of self-driving vehicles. These behaviours are extracted from the ns-2 trace file that were created by Simulation of Urban Mobility Model (SUMO) and Mobility Vehicles (MOVE) to model the real-world communication environment.
- Improving the detection aspect and reducing the number of false rate for proposed IDS of self-driving vehicles by utilising and employing some technologies such as: POS, fuzzification, normalisation and uniform distributions.

The hybrid IDS (misuse and anomaly) is proposed to provide sufficient security environment to the external communication system of self-driving vehicles. It plays an important role in detecting different types of DoS: black hole, grey hole and rushing attacks. In other words, three IDS are proposed in this chapter to secure the VANETs from potential attacks. Each IDS has the ability to identify one or more types of DoS attacks which have direct and negative impact on passengers and drivers' life as well as sensitive information. We assume that all communications take place on secure channels.

3.1 The Framework of the Proposed IDS to Detect Black Hole Attacks

Malicious vehicles have a direct and negative impact on the communication system of the other vehicles in that radio coverage area. In this chapter, an intelligent intrusion detection system is designed to protect the external communication of self-driving vehicles. However, malicious vehicles can launch different types of attack on VANETs, including DoS, black hole, grey hole, rushing, wormhole and spoofing attacks. A security system depends on intelligent IDS for the external communication systems in driverless and semi-autonomous vehicles. It is based on dataset collected (trace file) generated from ns-2. The security systems are tested with fuzzified data and normal data to distinguish fuzzification role in enhancing the detection rate and reducing the number of false alarms. In addition, they are evaluated with the whole extracted features and/or with significant features that are generated by POS methods from ns-2 trace file.

3.1.1 IDS Based on the Trace File to Detect Black hole Attack

An intrusion detection mechanism is designed for VANETs to secure the external communication system for autonomous vehicles. These are relevant features that describe the normal or abnormal behaviour of vehicles. The IDS uses FFNN and fuzzified data to identify black hole vehicles. The IDS utilised the features extracted from the trace file as auditable data to detect and block the attack. In addition, a hybrid detection is proposed in this IDS to detect the attacks. The steps below explain the proposed IDS - methodology that was tested and evaluated with whole normal datasets.

A. Establishing Mobility and Traffic Model

A network simulator is utilised to measure and evaluate the proposed security protocols and algorithms performance in VANETs. The ns-2 required two software programs to establish real-world traffic and the mobility of normal/abnormal scenarios of self-driving vehicles. The software employed SUMO and MOVE [150]. The output files of these tools are mobility and traffic files for the self-driving vehicles; these files are used as input to the ns-2 [151]. Basically, mobility models are divided into three types: urban mobility models, rural mobility models and highway mobility models [103]. The Manhattan urban mobility model is employed in the proposed IDS because it is widely used in the scientific research area and it also gives the vehicles a great deal of flexibility to move in vertical and/or horizontal direction [152]. Figure 3.1 below presents the traffic and mobility scenario for self-driving vehicles.

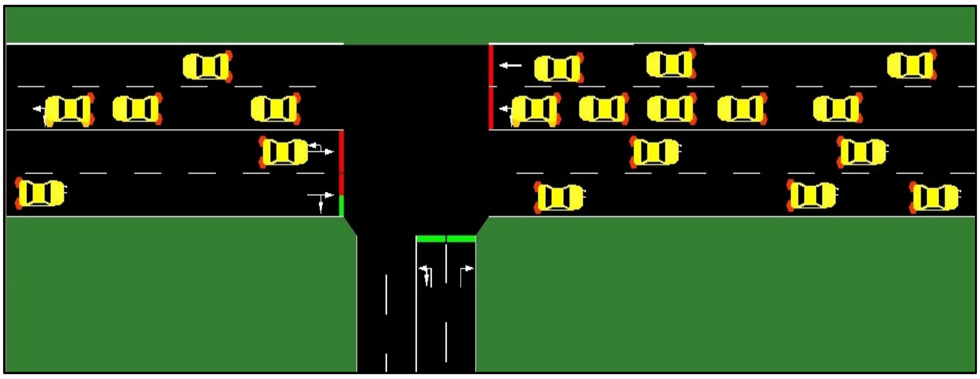


Figure 3.1 Traffic and Mobility Scenario.

B. Network Simulator Environment and Parameters

The external communication of autonomous vehicles environment is designed on the ns-2 simulator as shown in Figure 3.2 and one of the vehicles is established as a black hole vehicle. The ns-2 is built to simulate different networks, such as wired and wireless networks [88]. However, the researchers face a problem in simulating the VANETs with the ns-2 because the simulator is not designed specifically for VANETs. In this situation, the following extra tools or software are required to achieve the simulation: SUMO, MOVE and CityMob (generate mobility model) [150]. The network simulator (ns2.35-RC7) [88] and the mobility system are utilised to achieve the communication for VANETs in the real world. The VANET environment consists of 30 vehicles and six RSUs (30, 31, 32, 33, 34 and 35) on an ns-2 simulator in the proposed IDS [88].

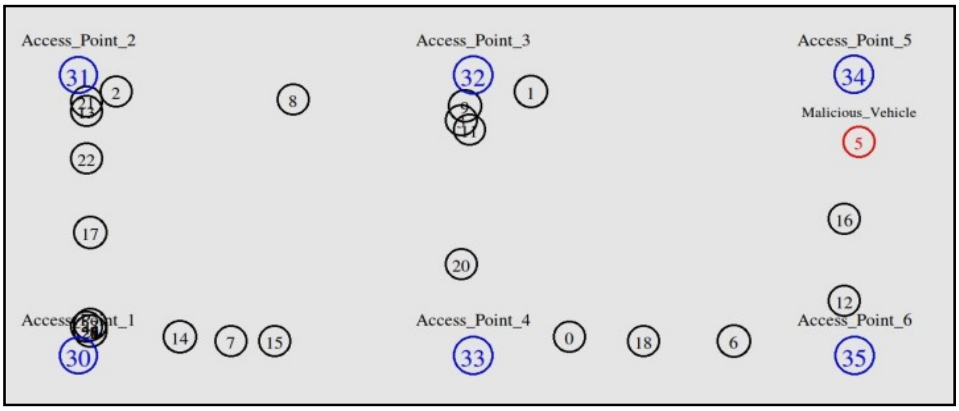


Figure 3.2 Screenshot of Simulation in ns-2 NAM.

The initial parameters of ns-2 are one of the important issues in the simulation system. They specify the performance and behaviour in the ns-2. Table 3.1 shows the parameters used in this design.

Table 3.1 Simulator Environment and Parameters.

Parameter	Value
Simulator	ns2.35
Simulation Time	250s
Number of Nodes	30 Vehicles
Number of RSUs	Six RSUs
Type of Traffic	Constant Bit Rate (CBR)
Topology	600 x 400 (m)
Transport Protocol	UDP/TCP
Packet Size	512
Routing Protocol	Vehicle-AODV, AODV and GPSR
Channel Type	Wireless
Queue Length	50 Packets
Number of Road Lanes	2
Radio Propagation Model	Two Ray Ground
MAC Protocol	IEEE 802.11p
Speed	50 m/s

Interface Queue Type	Priority Queue
Network Interface Type	Physical Wireless
Mobility Models	Manhattan Mobility Model

C. Generating Malicious Behaviour

In this scenario, normal and malicious behaviours are created in the proposed IDS. The malicious behaviour was generated in the ns-2 utilising the Object Tool Command Language (OTCL) script and Object Oriented Programming (OOP). In these scenarios, some files are required to modify/update in Vehicle Ad Hoc On Demand Distance Vector (V-AODV) routing protocol to generate the abnormal/malicious behaviour that was designed in the previous chapter. In this thesis, V-AODV routing protocol is utilised in designing the proposed security (that was described in detail in chapter two). The V-AODV protocol is a new version of normal AODV that was used in ad hoc networks. As mentioned in chapter two, this routing protocol can get better results as from normal compared to AODV and even GPSR routing protocol. The black hole vehicles dropped received packets rather than forwarding them to the destination vehicle in that radio coverage area as shown in Figure 3.3.

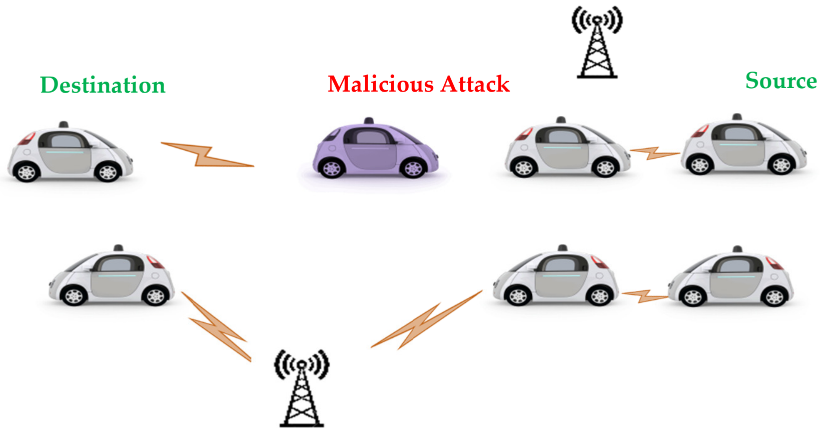


Figure 3.3 Malicious Attacks in VANETs.

3.1 The Framework of the Proposed IDS to Detect Black Hole Attacks

According to Figure 3.3, black hole vehicles dropped the received packets from source vehicles rather than forwarding it to the destination vehicle.

Various attack scenarios are explored in this thesis to assess the performance of proposed security systems, such as black hole, grey hole, rushing and flooding attacks. More specifically, flooding and dropping (black hole, grey hole and rushing) attacks are utlised to measure the performance efficiency in detecting abnormal behaviour. In one hand, dropping attacks such as black hole, grey hole or rushing are designed at network layer of wireless communication. In addition, these attacks scenarios are built on routing protocol files. In this case, routing protocol traces need to modified or updated to generate abnormal behaviour. On the other hand, TCL scenario files of ns-2 are modified to generate flooding, wormhole and Sybil attacks. However, we do not need to update routing traces to create these attacks. Therefore, the generation process for these attacks are increases or decreases the number of packets between source and destination, duplicates vehicles IDs and establishes tunnel connections between two vehicles in that radio coverage area. The dropping attacks scenario is shown in example 3.1 below.

Example 3.1:

Abnormal vehicles are added in ns-2 utilising VAODV routing protocol. These vehicles are have an abnormal behaviour that will drop sent/received packets between source and destination. This processor is required to modified two files of VAODV which are VAODV.h and VAODV.cc.

1. VAODV. h: abnormal vehicles are declared as a Boolean variable in the protected scope of the class VAODV.

```
{……..

bool abnormal;
```

……….}

2. VAODV. cc: in this file, we need to add the statement below to creating abnormal behaviour.

a. The dropping statement is added to "if (argc==2)" of VAODV.cc in routing protocol:

```
if (strcmp (argv[1], "abnormal") == 0) {
# t= true value.
abnormal = t;
return TCL_OK;
}
```

b. Constructor: false value of vehicles is initialised for abnormal vehicles and these values are declared inside the constructor section on VAODV:

```
VAODV::VAODV(nsaddr_t id):Agent(PT_VAODV)...
{
.......
Abnormal_behaviour = false;
}
```

c. rt_resolve(Packet *p) function: the abnormal behaviour of vehicles is implemented by including the statement below inside this function. Here, the abnormal vehicles will easily drop the received packets from any surrounding vehicles in that zone.

```
# t= true value.
if(abnormal_behaviour==t)
{
drop(p,DROP_RTR_ROUTE);
}
```

3. TCL script: in this script, abnormal vehicles are set by add the command below:

   $ns at 3.0 "[$node6 set ragent_] abnormal"

The abnormal behaviour of vehicles is shown in example 3.1. This example reflects malicious behaviours of black hole, grey hole and rushing attacks with different parameters, place of dropping attacks and time.

D. Dataset Source Collection

The accuracy detection rate of the IDS relies heavily on the number and types of features that describe the events in the VANET. The behaviour of vehicles is extracted from the trace file as it contains many different items of data (features) that can be utilised in the analysis. These features reflect the normal and abnormal/malicious behaviour in VANETs for self-driving vehicles.

A trace file is employed to evaluate the performance of the proposed intelligent IDS. It describes the VANET events that can be used for performance evaluation. For example, the number of packets transferred between two vehicles, the delay in the transfer of the packets, time, and packet drop. In this case, the type and the number of features are very important for efficiency of the IDS. The proposed IDS is trained and tested with whole features extracted from the trace file that describe the normal and malicious behaviour.

In addition, the trace file of V-AODV is clarified in more detail in Figure 3.4. The trace file in ns-2 is divided into three parts: basic trace, IP trace and V-AODV trace. Figure 3.4 below presents the contents of the trace file [153].

```
“r 20.0013554_31_MAC ------ 0 V-AODV, GPSR or AODV 48 [0 ffffffff 0 800] ------[0:255-1:255 30 0] [ 0x2 1 1 [1  0] [ 0  4] ]”
```

Figure 3.4 Trace File of ns-2.

Basic Trace Information:

- Event: r: receive; s: send; f: forward; D: drop.
- Timestamp: 20.0013554 s.
- Send node No. 31.
- The level of trace is at the "MAC" layer, RTR (network) and AGT (application).
- Flag: --------.
- The packets have a unique ID such as "0" in this record, payload type "V-AODV" and packet size "48" bytes.
- The delay time is "0".
- The MAC addresses of the source and the destination are "0" and "fffffff" respectively.
- The internet protocol (IP) works over an Ethernet (i.e., "800").

IP Trace File:

- The values of "0" and "1" are IP source and destination addresses respectively. The value of "255" represents the port value of source and destination.
- The time live is "30".
- The address of the next hop is "0".

V-AODV Trace:

- The value of "0x2" is tagged with the REQUEST packet.
- The value of "1" represents the number of hop counts, "1" is broadcast ID.
- The destination IP is "1".
- The sequence number is "0".
- The source IP is "0".
- The sequence number is "4".
- The string "REQUEST" confirms that the packet is RREQ.

The trace file contains 22 features which are shown in table 3.2 below [20].

Table 3.2 Features of the ns-2 Trace File.

Basic Trace	IP Trace	AODV Trace
Event, Time, Trace Level, Node Number, Packet ID, Payload Size and Type, Delay, Source and Destination MAC, IP Packet and Ethernet	IP Source and Destination, Time to Live and next Hop Node	Packet Tagged, Hop Counts, Broadcast ID, Destination IP with Sequence Number and Source IP with Sequence Number

To approve the detection efficiency, the proposed IDS is tested with a different dataset such as Kyoto dataset.

E. Pre-processing Data Set

The dataset benchmark is utilised to assess performance of the proposed IDS. This dataset needs three preprocessing stages which are: encoding, uniform distribution and normalisation.

- **Encoding st*age***: In this stage, some features were represented by symbols/letters such as event, routing protocol and level of trace with symbols: “r”, “AGT”, “RTR”. The proposed intelligent detection system deals only with numerical values. In this case, the security system needs to convert symbol features to numerical values before making any changes to the data set.
- **Uniform distribution stage***:* This stage is important with machine learning (FFNN and SVM), in order to ensure accurate training and testing. In this security system, 60.000 data set records are prepared to simulate the proposed security system. It is divided into three subsets with each of them using a different number of normal and abnormal records that were generated randomly from the original dataset benchmark. This distribution

is important for training and testing subsets that have different ratio of classes because the proportion of each subset (sample) per class is not of uniform distribution [154]. For example, the subset_1 in training phase contains 9861 normal records out 10000 records. Here, the ANN or SVM will not work very well in detection abnormal classes because it is not trained with sufficient number of abnormal class. In addition, this distribution effectively adapt with dataset that continuous probability distribution as well as observations ranging between 0.0 and 1.0 [155]. All these aspects of the dataset make a uniform distribution more suitable for the dataset extracted from trace file of ns-2. In more detail, they possess the following property: if the sample number of abnormal pattern is T subset and the original dataset has D samples, then there is a probability of finding a sample of class abnormal in the first subset D/T samples of the final dataset. Hence, each subset of the final data set has almost the same distribution and ratio of record type of the full data set.

- **Normalisation of numerical attributes stage***:* Each numerical feature is a value set between 0.0 and 1.0 according to Equation 3.1. Artificial neural network training is often more efficient with normalised data; it is used as the preferable predictor.

$$X = \frac{x - min}{max - min} \qquad (3.1)$$

where X is the normalised value with a range between 1.0 and 0.0, x is the original dataset value, max and min are maximum and minimum values of the original variable. These values are utilised to match the upper and lower limits of the activation Function-Sigmoid that has been used in the FFNN models. In the training phase, a subset of data was set aside for the purpose of validation which is a common problem in FFNN. It is over-fitting that usually occurs during the training phase. The stopping condition in training phase is when validation errors increase for a specified number of iterations.

F. Intelligent Detection System

The intelligent detection system uses a Feed Forward Neural Network (FFNN) to identify and block malicious vehicles in VANETs. Current research in the area of self-driving vehicles confirms that the FFNN is the most efficient and convenient in the design of internal and external systems for these vehicles [156]. The proposed IDS (32.000 data set records) describes the behaviour in the network and whether it is normal or malicious. The data set is divided into three subsets: the first subset is the training set (50%), the second subset is the validation set (25%) and the third subset is the test set (25%).

The stopping condition of the training phase is when the value of least-square-error is between the desired and the actual output is less than $E_{max=}$ $1*10^{-5}$. Figure 3.5 shows the basic structure of the FFNN.

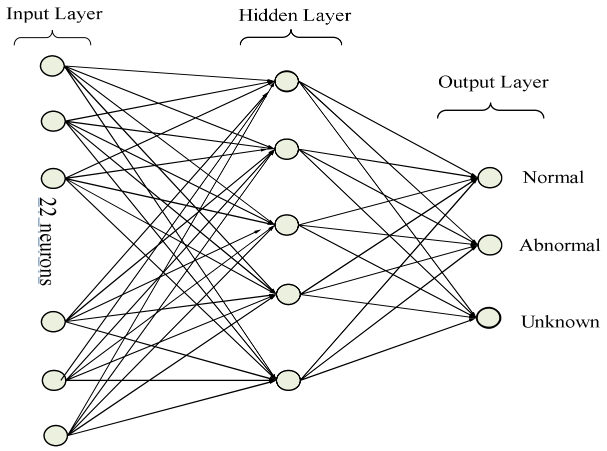


Figure 3.5 The Basic Structure of the Feed Forward Neural Network.

In this chapter, trial and error principle is employed to select the best configuration of FFNN. In other words, it is based on the best ratio of training depending on the condition in the second phase of the proposal. Figure 3.5 shows the network of FFNNs selected in this proposed IDS. The MATLAB R2016a toolbox provides neural network implementation in the proposed security system. Table 3.3 presents some of the configuration parameters used in the ANN.

Table 3.3 Feed Forward Neural Network Parameters.

Parameter	Values
Training Parameter epochs	68
Training Parameter learn	$1*10^{-5}$
Training Parameter goal	0
Training Parameter min_grad	$1*10^{-14}$

The initial parameters of FFNN play an important role on training accuracy and consumption time in training phase of the proposed security system. In this system, the epoch parameter is established with 500 epochs as stopping condition but according to Table 3.3, we note that ANN obtained an acceptable training rate with 68 epochs. As for the other parameters obtained in Table 3.3 and number of hidden layer are placed according to the trial and error principle with 98.97% average training rate. The simulation is based on a system with an Intel 5744 core i3-380M processor "2.53GHZ" and 4 GB RAM memory.

G. The Proposed Model of Intrusion Detection System

In this proposal, the ANN comprises of three layers: input, hidden and output. The input layer consists of 22 neurons equal to the number of the extracted features from the trace file. The hidden layer consists of five neurons while the output layer consists of three neurons. The proposed system has three stages and Figure 3.6 shows the overall architecture of the proposed IDS, namely:

- The first stage (Creating the mobility and the traffic model): Both "SUMO and MOVE" are utilised to generate the suitable scenarios for ns-2. The output files are considered input files for the ns-2.
- The second stage (ns-2): The ns-2 is employed in generating normal and malicious behaviours for vehicles. Two output files are obtained from ns-2 which are: text file (trace) and virtualisation (NAM) files. The IDS dataset is extracted from the ns-2 trace file.
- The third stage (data collection and pre-processing): The normal and malicious behaviour of the vehicles is designed into the ns-2 and a data set is generated from the trace file. The whole features are extracted from the data in the trace file. The extracted features are pre-processed using normalisation, transformation and uniform distribution. The normalisation converts all values between 0 and 1 that are extracted from network to increase the efficiency of FFNN.
- The fourth stage (training): The ANN is trained with the extracted data set (features).
- The fifth stage (testing): The ANN is tested with data features that describe malicious and normal behaviour. When the trained ANN is stable, it can survey the security of the VANETs by identifying the network control messages and data packets in real time and immediately generating an alarm if there is any malicious behaviour.

The malicious vehicles can perform many types of attacks, such as DoS attacks [157], and a detection system is built to detect the DoS attack. The DoS attack is detected through its behaviour such as dropping packets [72].

3.1 The Framework of the Proposed IDS to Detect Black Hole Attacks

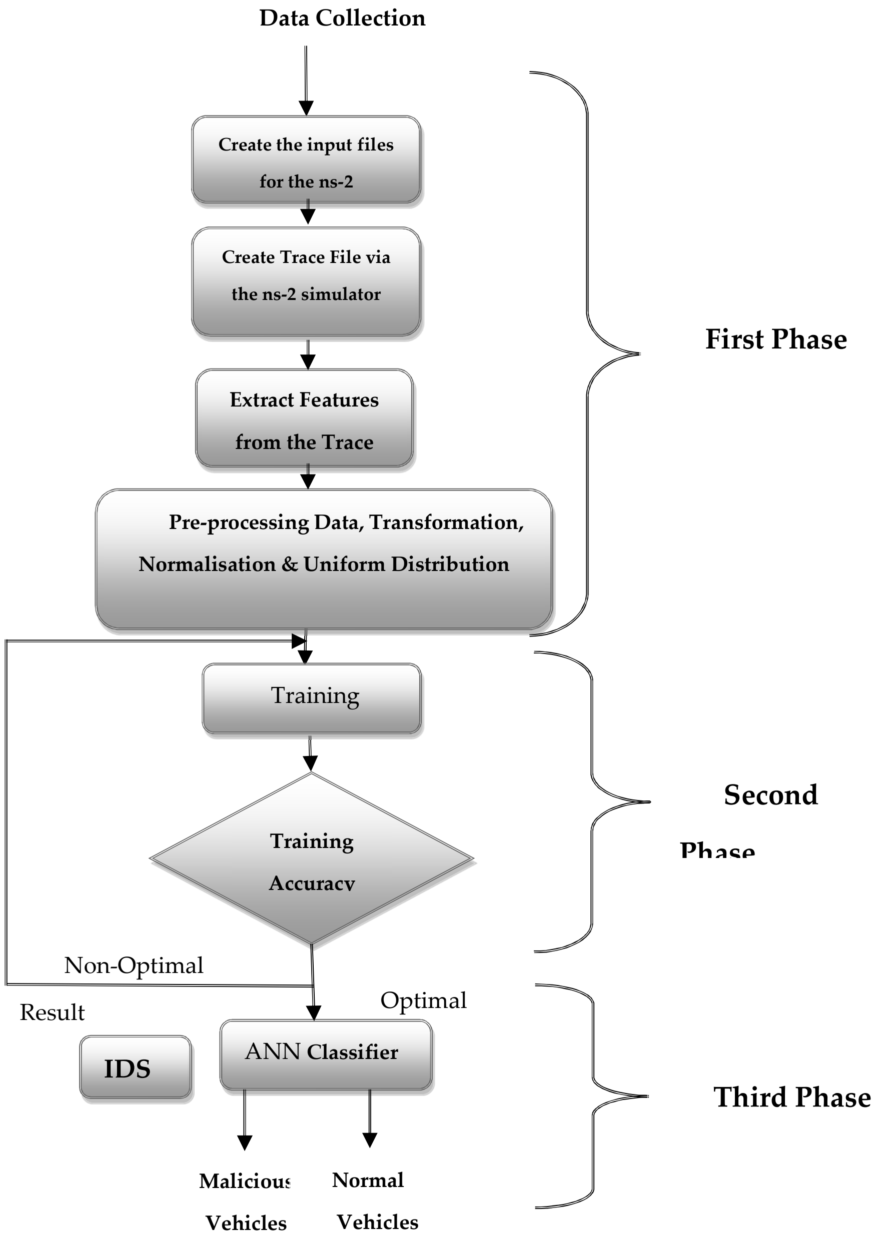

Data Collection
Create the input files for the ns-2
Create Trace File via the ns-2 simulator
Extract Features from the Trace
Pre-processing Data, Transformation, Normalisation & Uniform Distribution
First Phase
Training
Training Accuracy
Second Phase
Non-Optimal
Result
Optimal
IDS
ANN Classifier
Malicious Vehicles
Normal Vehicles
Third Phase

Figure 3.6 Architecture of IDS.

The main reasons for using the ANN are to reduce costs, to achieve real-time responsiveness and to be efficient [156].

3.1.2 Experimental Result

The intelligent detection system may be installed in three configurations: vehicles, RSUs, or both. The detection system in this IDS is configured in self-driving vehicles.

The security system can identify two different behaviours through the IDS: normal or abnormal/malicious.

The detection rate and four alarms are employed as a performance metric to evaluate the IDS. To measure and evaluate the performance of the IDS, four types of alarms are needed to calculate: true positive (TP), false positive (FP), true negative (TN) and false negative (FN). The accuracy of the detection can be calculated as follows [158]:

$$Accuracy = \frac{Number\ of\ correctly\ classified\ patterns}{Total\ number\ of\ patterns} \tag{3.2}$$

In addition, the measures will be calculated as follows [159]: Let

$$TP -\ normal\ connection\ record\ classified\ as\ normal$$
$$TN - \#\ attack\ connection\ record\ classified\ as\ attack$$
$$FP -\ normal\ connection\ record\ classified\ as\ attack$$
$$FN -\ attack\ connection\ record\ classified\ as\ normal:$$

$then$

$$TP_{Rate} = \frac{TP}{TP + FN} \tag{3.3}$$

$$TN_{Rate} = \frac{TN}{TN + FP} \tag{3.4}$$

$$FN_{Rate} = \frac{FN}{FN + TP} \tag{3.5}$$

$$FP_{Rate} = \frac{FP}{FP + TN} \tag{3.6}$$

In addition, the performance metrics are calculated for VANETs with or without the intelligent IDS for self-driving vehicles, such as PDR, average end-to-end delay and average throughput [160].

1. **Packet Delivery Rate (PDR):** It is the ratio between the numbers of packets generated or sent from the source vehicle and the ratio of packets received at the

destination vehicle. Figure 3.7 shows the PDR for VANETs with and without the IDS.

$$\text{PDR} = \frac{\Sigma\ Number\ of\ Packets\ Received}{\Sigma\ Number\ of\ Packets\ Sent} \tag{3.7}$$

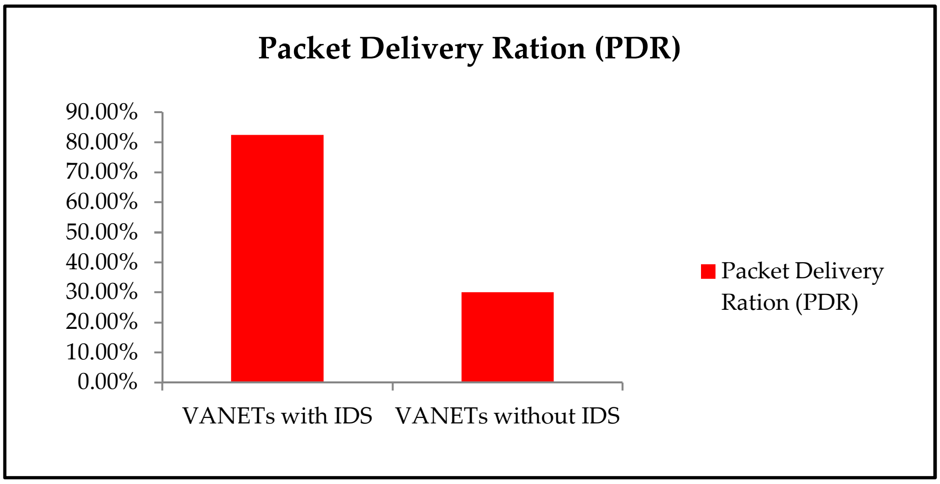


Figure 3.7 PDR for VANETs.

2. **Throughput:** It is the total number of packets that are transferred in the VANETs. This metric is used to calculate the effectiveness of the routing protocol in VANETs. Figure 3.8 shows the throughput for VANETs with and without the IDS.

$$Average\ Throughput(kbps) = \frac{number\ of\ received\ packets * packet\ size}{Simulation\ Time} \tag{3.8}$$

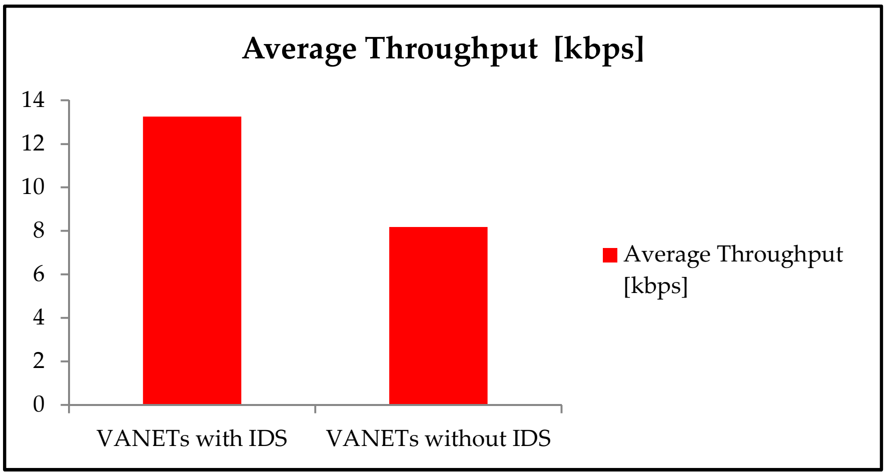


Figure 3.8 Average Throughput for VANETs.

3. Average End-to-End Delay: This metric is used to calculate the average packet delay based on time. In other words, the average time for the packets to reach from source to destination. Figure 3.9 shows the average end-to-end delay for VANETs with and without the IDS.

$$Average\ End - to - End\ Delay\ (ms) = (\frac{\sum end_{time} - start_{time})}{\sum Number\ of\ Connections} \qquad (3.9)$$

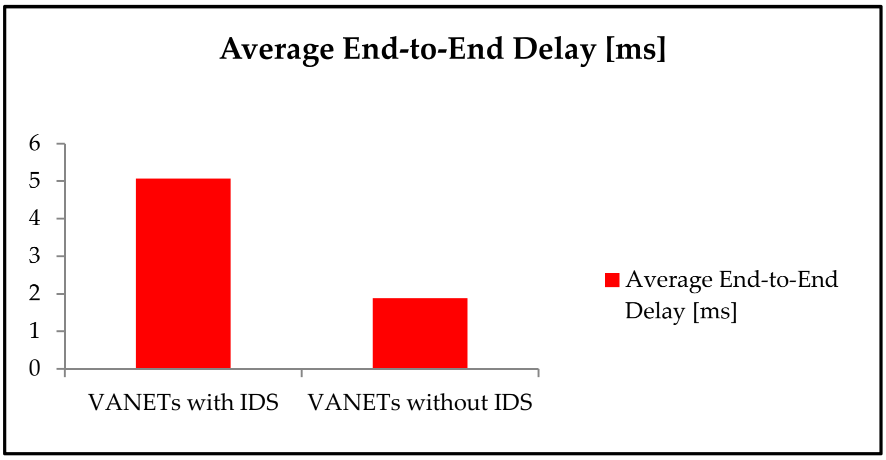


Figure 3.9 Average End-to-End Delay for VANETs.

The proposed IDS plays a vital role on the VANETs. Table 3.4 shows PDR, average throughput and average end-to-end delay for packets in VANETs.

Table 3.4 Performance Metrics for VANETs.

Performance	VANETs with IDS	VANETs Without IDS
Packet Delivery Ratio	82.50%	30%
Average Throughput [kbps]	13.25 *kbps*	8.19 *kbps*
Average End-to-End Delay	5.06 *ms*	1.88 *ms*

Figure 3.10 shows the number of sent, received and dropped packets in the external communication systems.

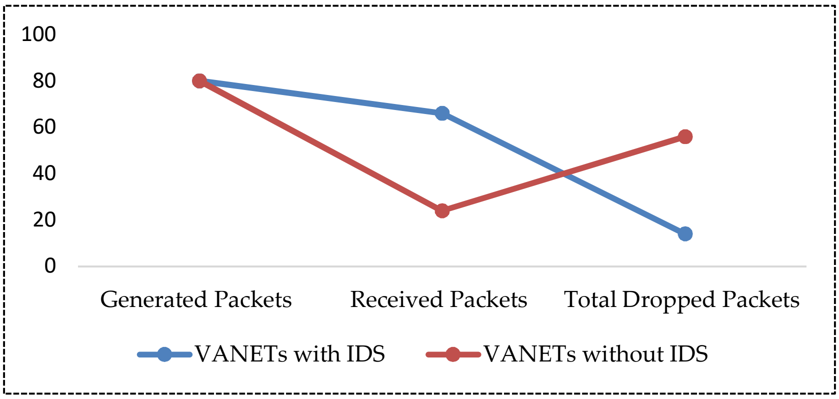


Figure 3.10 Number of Sent, Received and Dropped Packets in VANETs.

3.1.2.1 Results of Training and Testing the Neural Network (Misuse Detection)

During the training and testing phases, the same data set is utilised in both phases (signature) to calculate the total accuracy, true positive, false positive, true negative and false negative. The total accuracy of the training is 98.97%.

Figures 3.11 show the performance of the neural network.

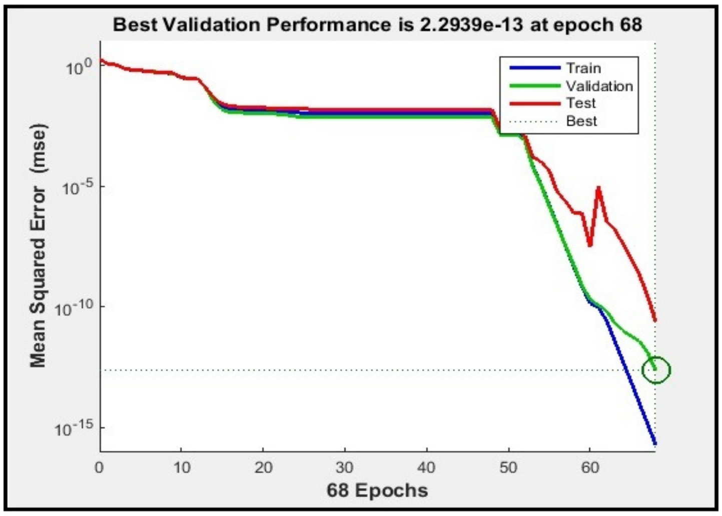


Figure 3.11 Training Performance of ANN.

The performance of the classification and the number of records utilised in the proposed system are shown in Table 3.5.

Table 3.5 Accuracy of ANN – IDS Classification.

IDS					
Classifica	Original	ANN	Match	Miss	Accurac
Normal	14533	14404	14379	25	98.94%
Abnormal	2868	2997	2843	154	99.12%
Unknown	0	0	0	0	NaN

The recognition rates are calculated using Equations 3.3, 3.4, 3.5 and 3.6 as shown in Table 3.6.

Table 3.6 Recognition Rate of ANN-IDS.

Alarm Type	Accuracy
True positive	99.82%
True negative	94.86%
False negative	0.17%
False positive	5.13%

3.1.2.2 Results of Training and Testing the Neural Network (Anomaly Detection)

During the training and testing phases, the data set utilised in the testing phase differs from the data set used in the training phase (anomaly). The detection accuracy is calculated to evaluate the performance of the IDS. In this case, the IDS must be able to detect novel attacks. The performance of the classification and the number of records used in the proposed system are shown in Table 3.7.

Table 3.7 Accuracy of IDS Classification.

IDS					
Classifica	Original	ANN	Match	Miss	Accuracy
Normal	28676	28790	28234	556	98.45%
Abnormal	3725	3609	3167	442	85.02%
Unknown	0	2	0	2	NaN

The recognition rates are calculated using Equations 3.3,3.4, 3.5 and 3.6 as shown in Table 3.8.

Table 3.8 Recognition Rate of ANN-IDS.

Alarm Type	Accuracy
True positive	98.06%
True negative	87.75%
False negative	1.93%
False positive	12.24%

3.1.3 System Analysis

The motivation behind the proposed IDS system is to implement secure communication in self-driving vehicles by identifying malicious vehicles in VANETs. This system is implemented in five phases: Creating mobility and traffic model, establishing vehicles behaviours via ns-2, data collection and pre-processing, training, and testing.

The experiments in the ns-2 and MATLAB show that the detection system is effective and efficient in identifying anomalies with a low false negative alarm rate. The error rate is 2.05%. The obtained results indicate that the calculated rate of alarms fluctuate between 94.86% and 99.82% which involves efficient accuracy detection. On the other hand, the anomaly detection system has a low false negative alarm rate of about 2% which is a good indicator of the results. However, the problem is the high rate of false positives in the anomaly detection because of the different records that describe both normal and abnormal behaviour.

The IDS is formally discussed in a research paper [20] which was presented at the 12th International Conference on Consumer Communications Networking: CCNC 2015 workshops–IEEE CCAN, 978-1-4799-6390-14/15 IEEE, Las Vegas, Nevada, USA, 2015.

3.2 IDS based on the Significant Features from Trace File to Detect Drooping Attacks

An intelligent security system is proposed for the VANETs of self-driving vehicles that is based on an intelligent IDS. The security system relies on the features of trace file that is generated from the ns-2. In this security system, the proposed IDS is based on significant features extracted by the POS method from the trace file of routing protocol. In addition, the IDS is trained and tested with fuzzified dataset. Generally, the steps are the same as utilised in the previous IDS. In this case, the outline of the steps without any details is mentioned, but some of the contributions will be clarified in detail.

A. Feature Extraction

The number and type of extracted features have a vital and direct role in the effective and efficient performance of the proposed security system. To increase the efficiency of the detection system rate, the proposed IDS needs to extract the most effective features on which to base the security system. In this chapter, the IDS requires to evaluate and weigh each feature to reduce the number of features. A statistical approach is employed to extract the significant features that have a high weight value, using the POS method [161].

According to the current studies, many researchers have considered the POS method to be the most efficient even when the extracted dataset has many problems [149]. The identification features are selected by evaluating the overlap between the feature values across both "normal and abnormal" classes.

The POS method is utilised to measure the overlap rate between the features extracted in the ns-2 trace file [149], and shown below is the POS algorithm 3.1.

Algorithm 3.1 POS Method for Features Selection

```
1. For all features in $x$ and both the classes find inter quartile range and then based on it find features mask.
2. Compute POS as defined in [162] and assign each feature its domanial class.
3. Based on step 1 and 2 find aggregative features mask [162].
4. Find those features that correctly classify all observation in the training set based on step 3.
5. Arrange the rest of the features (exceeding those in the minimum set) with respect to POS and relevancy.
6. Add the top ranked features to the minimum set to get the full set of features.
```

21 features are extracted from the trace file and the statistical R language is used to implement the POS algorithm. Table 3.9 shows the POS order and value for each feature in the trace file.

Table 3.9 Features Extracted.

Feature No.	Feature Name	POS Value
1	Time	7.777406e-02
2	Trace Level	1.004217e-01
3	Node ID	1.105206e-01
4	Flag	1.207380e-01
5	Packet ID	1.504676e-05
6	Payload Type	0.000000e+00
7	Payload Size	0.000000e+00
8	Delay	6.922136e-02
9	Source MAC	0.000000e+00
10	Destination MAC	1.292744e-04
11	Ethernet	0.000000e+00
12	IP Source Address	6.161803e-02
13	IP Destination Add	8.132236e-06
14	TTL	1.393600e-02
15	Request Packet	1.139098e-05
16	No. Hop	0.000000e+00
17	Destination IP Add	0.000000e+00
18	Seq. Number	0.000000e+00
19	Source IP Address	2.187990e-04
20	Seq. Number	7.130718e-05
21	Tagged	0.000000e+00

The extracted features can redistribute in Table 3.9 that was based on the POS scheme to show the overlap of features. In this proposed security system, the POS applied 20 attempts to show overlap and generate the weight value for each feature extracted from the trace file. According to Table 3.10, the proposed IDS can select the 15 features that have a high value of POS and low repetition and overlap as well as significant roles in the detection system.

Table 3.10 Appearance of Features (as a percentage).

Feature No.	Feature Name	POS	Impressions	Percentage of appearance for feature selected
6	Payload Type	0.000000	20	100%
7	Payload Size	0.000000	20	100%
9	Source MAC	0.000000	20	100%
16	No. Hop	0.000000	20	100%
11	Ethernet	0.000000	20	100%
13	IP Destination Address	6.795097	20	100%
17	Destination IP Address	0.000000	20	100%
15	Request Packet	1.292640	20	100%
18	Seq. Number	0.000000	20	100%
5	Packet ID	1.803172	20	100%
21	Tagged	0.000000	20	100%
20	Seq. Number	6.492623	20	100%
10	Destination MAC	1.289860	20	100%
12	IP Source Address	6.164915	20	100%
19	Source IP Address	1.667554	9	45%
4	Flag	1.185719	5	25%
8	Delay	8.604373	3	15%
3	Trace Level	1.100107	2	10%
2	Node ID	1.003258	1	5%
1	Time	9.613269	0	0%
TTL		1.393555	0	0%

Table 3.11 shows the selected top 15 features identified by the largest weights after POS.

Table 3.11 Feature Selection.

Feature Selected	Feature Name	POS
6	Payload Type	0.000000e+00
7	Payload Size	0.000000e+00
9	Source MAC	0.000000e+00
11	Ethernet	0.000000e+00
16	No. Hop	0.000000e+00
17	Destination IP	0.000000e+00
18	Seq. Number	0.000000e+00
21	Tagged	0.000000e+00
5	Packet ID	1.504676e-05
13	IP Destination	8.132236e-06
15	Request Packet	1.139098e-05
20	Seq. Number	7.130718e-05
10	Destination MAC	1.292744e-04
19	Source IP Address	2.187990e-04
12	IP Source Address	6.161803e-02

To evaluate the 15 selected features, the trial and error principle is utilised to choose the perfect number of features based on the training accuracy. The proposed system began with an entire set of features. After each round of training, the features which had the lowest weight id were removed. The process was repeated until we are left with a set comprising only 15 features which was then used to classify normal and abnormal behaviour.

B. Fuzzy Set Membership

The data set extracted from the trace file “features” has a direct influence on the detection performance of the IDS [57]. When the detection system had a problem involving the distribution and nature of the features, or where the name of the classes was not well defined between normal and malicious behaviour, the detection rate is reduced and the number of false alarms in the IDS is increased. In this situation, a mathematical model is employed to redistribute the extracted features. In this research, a fuzzy set is employed to solve the problem of the data set. This was employed for a number of reasons; it is well known, widely used in scientific fields, and efficient [163].

The fuzzy set is a mathematical model used with data sets that have classification problems [149]. It is considered to be one of the most appropriate applications with classification problems as it applies fuzzification on the features extracted from the trace file "ns-2" [149]. Figure 3.12 shows the triangular membership function that was utilised in this proposed IDS [149].

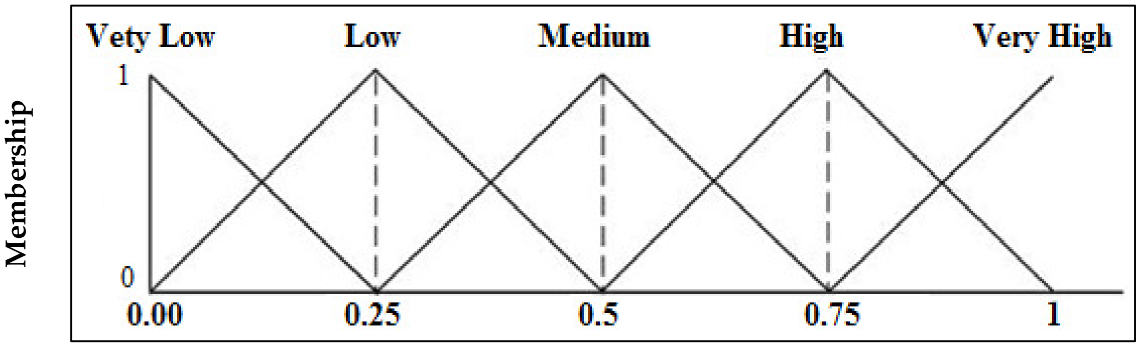


Figure 3.12 Fuzzification Data.

According to Equation 3.11, each single value from the data set is distributed in five values from the fuzzy domain and the range of intervals is [0, 1]. Linguistic expression is generated from linguistic notions [164].

$$f\left(x,a,b,c\right)=\begin{cases}0, & x\leq a\\ \dfrac{x-a}{b-a}, & a\leq x\leq b\\ \dfrac{c-x}{c-b}, & b\leq x\leq c\\ 0, & c\leq x\end{cases}\tag{3.10}$$

where a, b and c represent the fuzzy domain value distributed between the fuzzy set while x is the normal value of the data set before fuzzification. The motives for applying fuzzification data are that it enhances the detection rate of the IDS and reduces the number of false alarms generated by the IDS.

C. Simulation Parameters and Generating Malicious Vehicles

In this proposal, the VANET is an extended environment to nine RSU vehicles (40, 41, 42, 43, 44, 45, 46, 47 and 48) as shown in Figure 3.13 and selected two of them as Black hole vehicles.

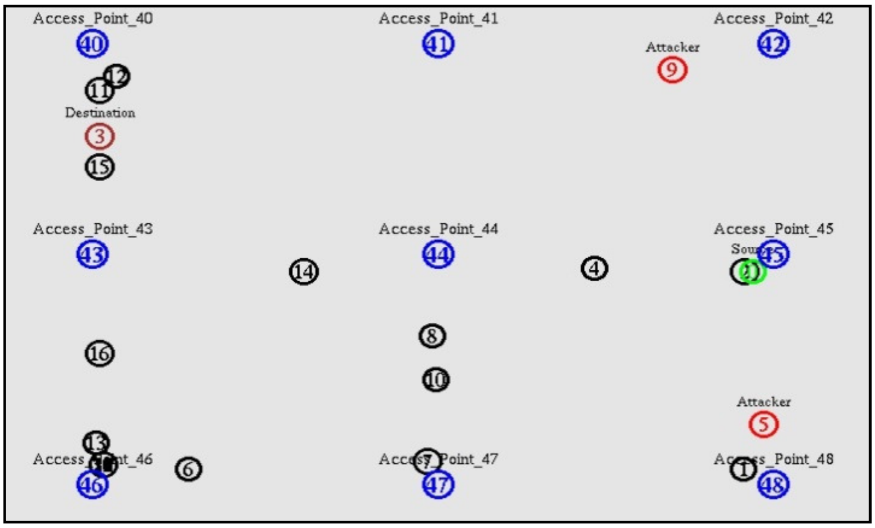


Figure 3.13 Screenshot of Simulation in ns-2 NAM.

Initial parameters are one of the most important issues in the simulation system. They determine the behaviour and performance in the ns-2.

Table 3.12 Simulator Environment and Parameters.

Parameter	Value
Simulator	NS2.35-RC7
Simulation Time	500s
Number of Nodes	40 Vehicles
Number of RSUs	9 RSUs
Type of Traffic	Constant Bit Rate (CBR)
Topology	650 x 450 (m)
Transport Protocol	UDP/TCP
Packet Size	512
Routing Protocol	V-AODV
Channel Type	Wireless
Queue Length	50 Packets
Number of Road Lanes	2
Radio Propagation Model	Two Ray Ground
MAC Protocol	IEEE 802.11Ext

Speed	30 m/s
Interface Queue Type	Priority Queue
Network Interface Type	Physical Wireless
Mobility Models	Manhattan Mobility Model

The intelligent IDS is required to change the parameters of the FFNN because it altered the training and testing data set (60,000 data set records) as well as adapt with new dataset. Table 3.13 shows some of the configuration parameters of the training phase of the FFNN.

Table 3.13 Feed Forward Neural Network Parameters.

Parameter	Value
Training Parameter epochs	15
Training Parameter Learn	$1*10^{-7}$
Training Parameter goal	0
Training Parameter min_grad	$1*10^{-12}$

The initial parameters of FFNN play important role on training accuracy and consumption time in training phase of the proposed security system. In this system, the epoch parameter is established with 500 epochs as stopping condition but according to Table 3.13, we note that the ANN obtained an acceptance training rate with 15 epochs. As for the rest of the parameters that mentioned in Table 3.13 and number of hidden layer are placed according to the trial and error principle with 99.86% average training rate.

D. The Proposed Intrusion Detection System

The proposed security system used a FFNN consisting of three layers: input, hidden and output. The first layer comprises 75 neurons, equal to the number of fuzzification features. The hidden layer has eight neurons while the output layer has three neurons, “normal, abnormal and unknown”. Figure 3.14 shows the overall architecture of the proposed security system, namely:

- The first stage (generate the mobility and traffic model): At this stage, both "SUMO" and "MOVE" are employed to generate the suitable scenarios for the ns-2. These files are considered to be input files for the simulation system.
- The second stage (ns-2): The normal and malicious behaviour for the vehicles was built. Two output files are obtained: trace and NAM. The data set was extracted from the trace file generated from the ns-2.
- The third stage (data collection and pre-processing): The features were extracted from the trace file. The features were pre-processed by converting them into numeric values and the values were normalised to values between zero and one. Normalising the data increases the detection rate and enhances the performance of the ANN [34].
- The fourth stage (extracting the significant features): In this stage, the significant features are extracted from the trace file. The POS was utilised to extract features that have a high priority value.
- The fifth stage (fuzzy set): The fuzzy set was employed to convert the selected features into their fuzzified counterparts to fix the overlap data set.
- The sixth stage (training phase): The FFNN was trained with the extracted data set (significant). A repeat condition was established at this stage to obtain the best ratio from the training. The raw data set was divided into six subsets, each subset containing 10,000 records. For each iteration of the training cycle, a different subset was used for training. Hence, the proposed system utilised three subsets (30,000 records) which resulted in an exceptional training rate of 99.86%.

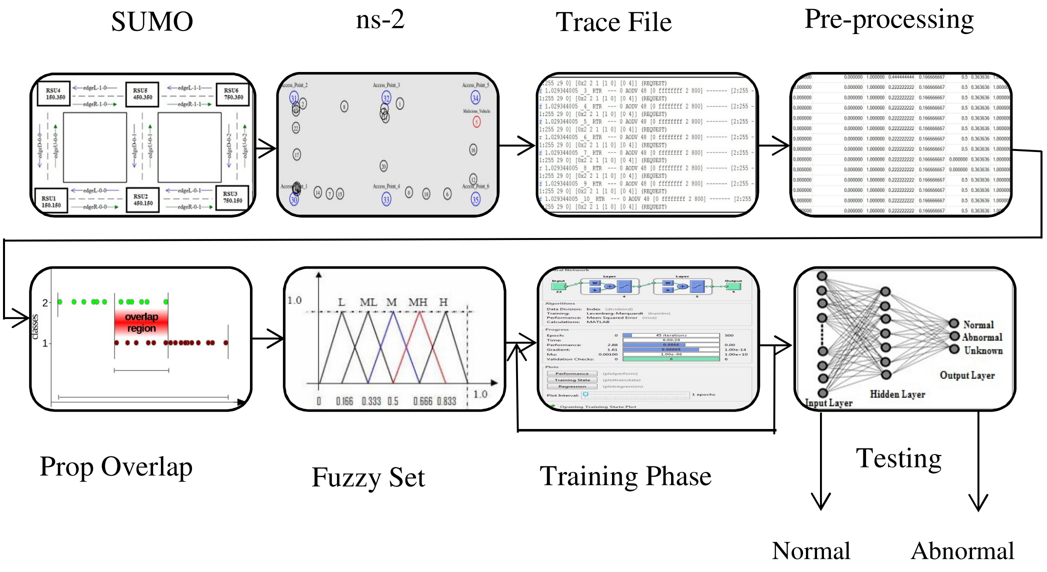


Figure 3.14 Architecture of the IDS.

The malicious vehicles can appear in many types of intrusions such as DoS, black hole, wormhole and grey hole attacks, and here a detection system is designed to identify the dropping attack. The black hole attack is detected by its behaviour that was designed in the ns-2 [165].

3.2.1 Experimental Results

The methodology utilised in the proposed security system was used in the previous proposal to generate the different types of alarm. The training and testing phases used the same fuzzification data set in both phases (signature) to calculate the total accuracy of the IDS, true positive, false positive, true negative and false negative. The total accuracy of the training is 99.86 %. Figures 3.15 show the performance of the neural network.

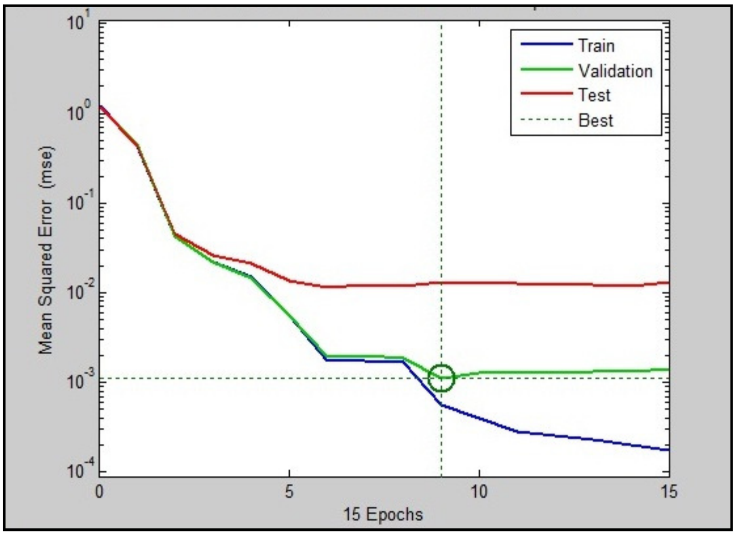


Figure 3.15 Training Performance of ANN.

The role of the proposed IDS is explained in the secure VANETs for self-driving vehicles by calculating the performance metrics, as in the previous proposal. Now, the proposed IDS needs to calculate PDR, average throughput and average end-to-end delay for VANETs with IDS and infected VANETs with drooping attacks. Using Equations 3.8, 3.9 and 3.10. Table 3.14 shows the performance metrics for VANETs.

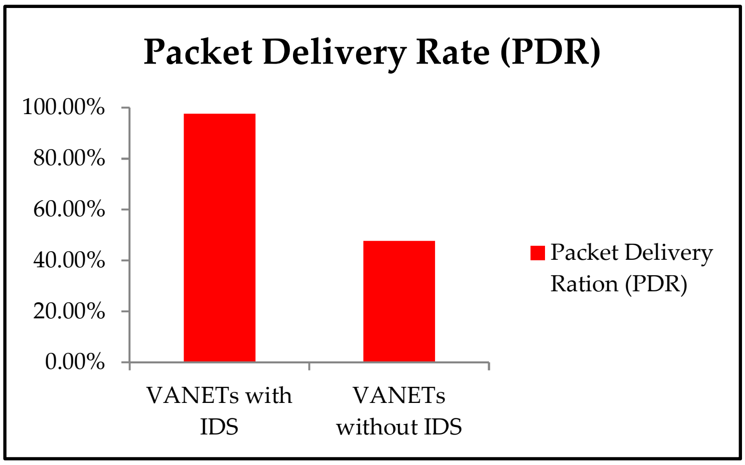


Figure 3.16 PDR for VANETs.

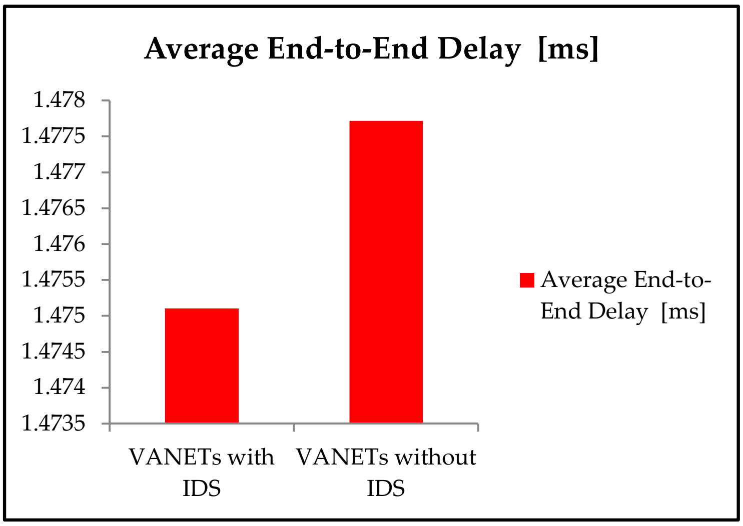


Figure 3.17 Average End-to-End Delay.

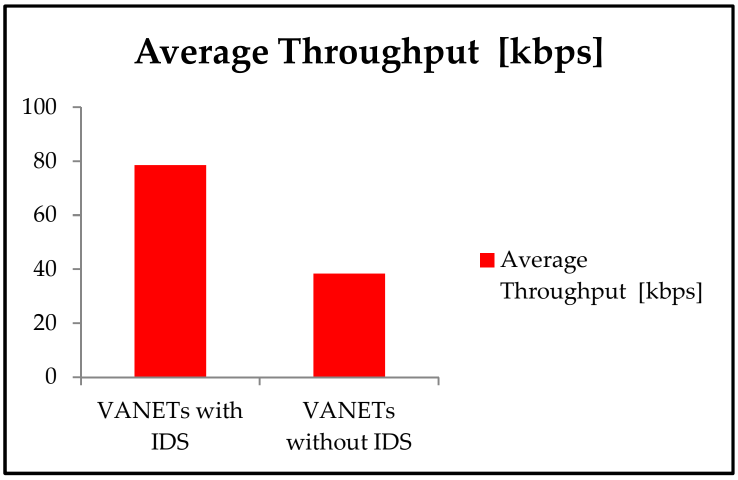


Figure 3.18 Average Throughput for VANETs.

Table 3.14 Performance Metrics for VANETs.

Performance Metrics	VANETs with IDS	VANETs Without IDS
Packet Delivery Rate	97.68%	48%
Average End-to-End Delay	1.4751*ms*	1.47772*ms*
Average Throughput [kbps]	78.57*kbps*	38.27

Figure 3.19 shows the number of sent, received and dropped packets in VANETs with and without the IDS. The important role is observed of the IDS in terms of the performance and throughput in the communication of self-driving vehicles.

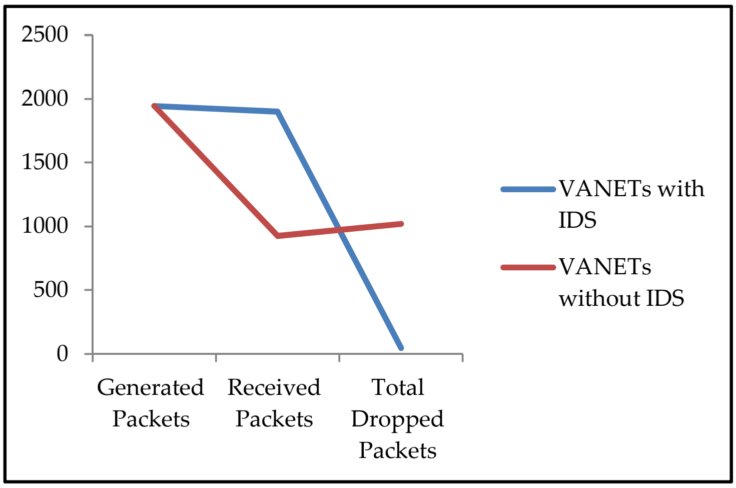


Figure 3.19 The Number of Sent, Received and Dropped Packets in VANETs.

3.2.1.1 Training and Testing the Neural Network (Misuse Detection Based)

The training and testing phase utilised the same fuzzification data set in both phases (signature) to calculate the total accuracy of the IDS, true positive, false positive, true negative and false negative. The total accuracy of the training classification was 99.8%. One subset (10,000 records) was used in the testing phase. Table 3.15 shows the performance of the classification system and the number of records of features used in the security system.

Table 3.15 Classification Rate of FFNN-IDS.

Intrusion Detection System					
Classifica	**Original**	**AN**	**Match**	**Miss**	**Accurac**
Normal	6382	6381	6375	6	99.89%
Abnorma	3618	3617	3611	6	99.80%
Unknown	0	0	0	2	NaN

The rates of alarm are calculated using Equations 3.3, 3.4 3.5 and 3.6 as shown in Table 3.16.

Table 3.16 Alarm Rates of FFNN-IDS.

Alarm Type	Accuracy
True positive	**99.90%**
True negative	**99.83%**
False negative	**0.09%**
False positive	**0.16%**

3.2.1.2 Training and Testing the Neural Network (Anomaly Detection Based)

The testing phase used a fuzzified data set that differs from the data set utilised in the training phase (anomaly). The total accuracy is calculated to evaluate the proposed security system. The anomaly detection system must be able to identify novel attacks. Three subsets (30,000 records) are utilised in the testing phase. Table 3.17 shows the performance of the classification and the number of records used in the IDS.

Table 3.17 Classification Rate of FFNN-IDS.

Intrusion Detection System					
Classifica	Original	AN	Match	Miss	Accurac
Normal	19285	19288	19261	27	99.87%
Abnorma	10715	10698	10685	13	99.72%
Unknown	0	14	0	14	NaN

Table 3.18 shows the rates of alarm calculated by Equations 3.3, 3.4, 3.5 and 3.6.

Table 3.18 Alarm Rates of FFNN-IDS.

Alarm Type	Accuracy
True positive	**99.86%**
True negative	**99.87%**
False negative	**0.14%**
False positive	**0.12%**

3.2.2 System Analysis

The proposed IDS is implemented in six phases: generating the mobility and traffic model, network simulation version 2, data collection and pre-processing, extracting the main features, fuzzification of the data, training and testing.

The experimental results confirm that the performance of the IDS is efficient in detecting dropping vehicles with a low false alarm rate. On one hand, the results indicate a high accuracy of detection rate, whether normal or abnormal, that fluctuate between 99.89% and 99.72% with a low error rate of 0.15%. On the other hand, the anomaly detection system is a good indicator of the results and it also has a low false alarm rate of about 0.14%.

In this research, the detection rate ranges between 99.72% and 99.89%. When comparing these results with our previous research where fuzzy sets were not used, a detection rate is obtained that ranged between 85.02% and 99.12% [106]. The percentage of false alarms ranged between 0.9% and 0.16%. When comparing these results with our previous research where fuzzy sets were not used, the obtained false alarm rate ranged from 0.17% to 12.24% [106]. According to the results, the differences are observed between the ratio of detection and false alarms. The use of a fuzzy set increases the detection rate while decreasing the number of false alarms. We can see from the previous studies that the proposed system has improved detection and has overcome the data set problems by applying the POS method in order to extract the significant features and perform a fuzzy set "fuzzification" on the data set which was extracted from the trace file. This scheme has a direct and positive impact on the result by increasing the detection rate and decreasing the false alarm rate and error rate. However, the main problem is that the system needs extra memory resources to store the data and the approach is computationally expensive. The low error rate indicates that the IDS is effective and efficient in identifying anomaly and misuse "hybrid detection" with high accuracy and a low false positive alarm rate. The proposed work can be extracted to build an IDS which can detect other types of attacks such as grey and wormhole attacks.

The proposed IDS was published in a research paper [166] at the 6th International Conference on Emerging Security Technology (EST-2015) - IEEE, Brunswick, Germany, 2015.

3.3 An IDS Based on the Trace File to Detect Grey hole and Rushing Attacks

In this work, the same research methodology was used as was mentioned in the previous proposal to detect the black hole attack. However, the main difference from the previous proposal is the type of attacks and the type of machine learning used in designing the intelligent IDS. In other words, it is based on the FFNN and SVM to detect the grey hole and rushing attacks. In this case, two types of detection system are designed and the two IDSs are compared to find out which would be more efficient.

In addition, the security system used the same features that were extracted from the previously proposed system based on the POS approach to extract the significant features. Fuzzification is applied on the extracted features from the trace file to increase the detection rate and decrease the number of false alarms. The steps below explain the methodology of the proposed security system.

A. **Network Simulation Parameters and Mobility Scenarios**

The same infrastructures and vehicles are used as in the previously proposed IDS to detect Black hole attacks as shown in Figure 3.20. There are four malicious vehicles, two vehicles with grey hole attacks and two with rushing attacks. The Manhattan mobility model (Mmm) is used in this proposed IDS. It is considered to be a type of urban mobility model [88]. In addition, the same parameters are used as in the previous IDS.

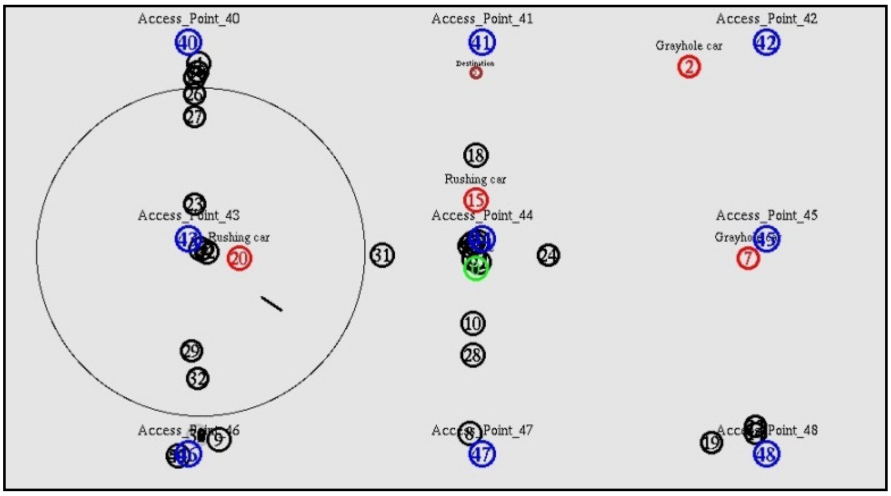


Figure 3.20 Screenshot of ns-2.

B. **Intelligent Security System**

The intelligent IDS based on a FFNN is designed to detect grey hole and rushing vehicles in the external communication system. Many recent studies have focused on the ANN as the most efficient in building internal and external systems for self-driving vehicles [156].

The proposed IDS utilised 40,000 data set records to describe the normal and abnormal behaviour in VANETs. The data set collected from the trace file was divided into three subsets: the test set (25%), the validation set (25%) and the training set (50%) to avoid one of the most common problems of an ANN which is the overfitting by specific parts of the data set to validation.

To select the best configuration of the ANN, the trial and error principle is used to configure and select the best ratio of training depending on the condition put in the seventh and eighth phases of the proposal. Figure 3.21 shows the best structure of the ANN that was selected in our proposal.

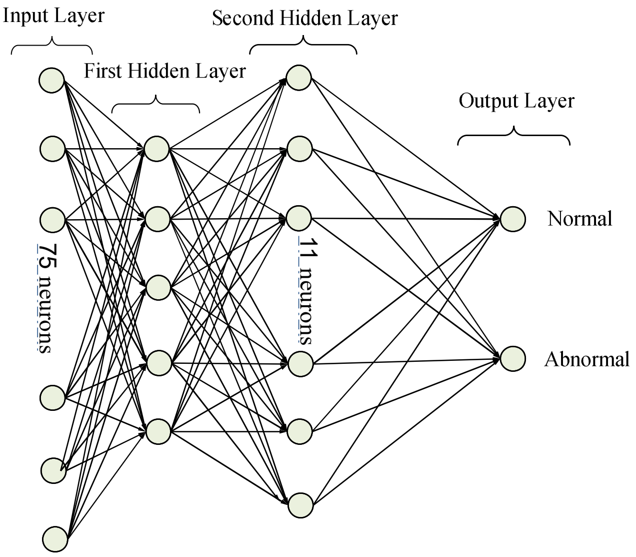


Figure 3.21 Structure of the FFNN.

The learning parameter is considered to be one of the most important parameters in the ANN [167]. The ns-2 parameters have an important role in the performance of the FFNN that have a direct impact on the performance of detection. Table 3.19 shows some of the initial parameters of the training phase utilised in the FFNN and SVM.

Table 3.19 Artificial Neural Network Parameters.

Parameter	Value
Training Parameter epochs	46
Training Parameter learn	$1*10^{-8}$
Training Parameter goal	0
Training Parameter min_grad	$1*10^{-13}$
Gaussian Radial Basis Function	1
BoxConstraint	1e5

The initial parameters of FFNN play important role on training accuracy and consumption time in training phase of the proposed security system. In this system, the epoch parameter is established with 500 epochs as stopping condition but according to Table 3.19, we note that ANN obtained an acceptance training rate with 46 epochs. As for the rest of the parameters that mentioned in Table 3.19 and number of hidden layer are placed according to the trial and error principle with 98.24% average training rate.

C. The Proposed Intrusion Detection System

Machine learning has an important role in enhancing the performance of the proposed IDS. For this reason, two types of machine learning (FFNN and SVM) are utilised in the design of the proposed IDS to detect two types of attack in VANETs – grey hole and rushing vehicles. These malicious vehicles have a direct and negative impact on all the vehicles in that particular zone. In this research, the ANN consists of an input layer, a hidden layer and an output layer. The input layer comprised 75 neurons equal to the fuzzification features after applying a fuzzy set to them. Two hidden layers are designed in this proposal to increase the accuracy of the detection system and to decrease the number of false alarms. The first hidden layer consisted of five neurons and the second hidden layer consisted of 11 neurons while the output layer consisted of two neurons, "normal and abnormal". The proposed IDS has eight stages and the overall architecture of the proposed security system is shown in Figure 3.22, namely:

- The first stage (generate the realistic world): In this stage, two tools are required to generate the mobility and traffic model that reflected the real movement of vehicles in the external communication system. These tools are SUMO and MOVE.
- The second stage (ns-2): The output files from the first stage are utilised as input files in the ns-2. In this stage, normal, grey hole and rushing attacks are simulated to generate two files. These files are the trace file and the NAM file.
- The third stage (data extraction): In this stage, all the features from the trace file are extracted that were generated in the second stage. However, the proposed system only used 15 significant features from all the features [166]. In addition, reducing

the number of features has a vital role in increasing the detection rate and decreasing the false alarms.

- The fourth stage (pre-processing): In this stage, the extracted features required some pre-processing techniques such as transformation to convert some letters and symbols to numbers, and a uniform distribution to balance the different types of classes in collecting the data to increase the efficiency of the detection rate and normalisation process to convert all the values of the features between zero and one to make the performance of the FFNN more efficient.
- The fifth stage (fuzzy set): In this stage, fuzzification data set was generated from the normal data. This process can solve some of the common classification problems that occur in the data set such as overlap and a lack of clarity.
- The sixth stage (training and testing phase – FFNN): The FFNN is trained and tested with the extracted data that was produced in the fifth stage. In this stage, the detection rate is obtained for normal/abnormal behaviour, and four types of alarm are calculated.
- The seventh stage (training and testing phase – SVM): The SVM with fuzzification data is trained and tested that was extracted in the fifth stage to check the efficiency of the proposed security system in the detection of grey hole and rushing vehicles in comparison to normal vehicles.
- The eighth stage (comparison): In this stage, the two proposed intrusion detection systems are compared that are based on FFNN and SVM to check which was more efficient based on the criteria to make these decisions, such as detection rate and the number of false alarms.

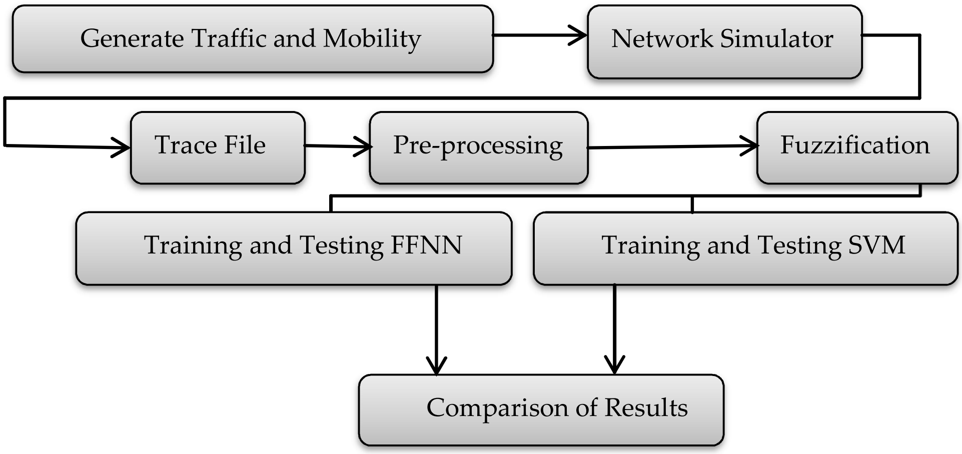


Figure 3.22 Architecture of IDS.

3.3.1 Experimental Results

Two types of self-driving vehicle scenarios are generated under certain conditions in order to obtain real data. This data was processed to extract the significant features with some pre-processing of the data. In this case, the proposed systems have ready data for training and testing to measure the performance of the proposed intelligent detection system. The total accuracy of the training is 98.24%. Figures 3.23 show training status of the neural network.

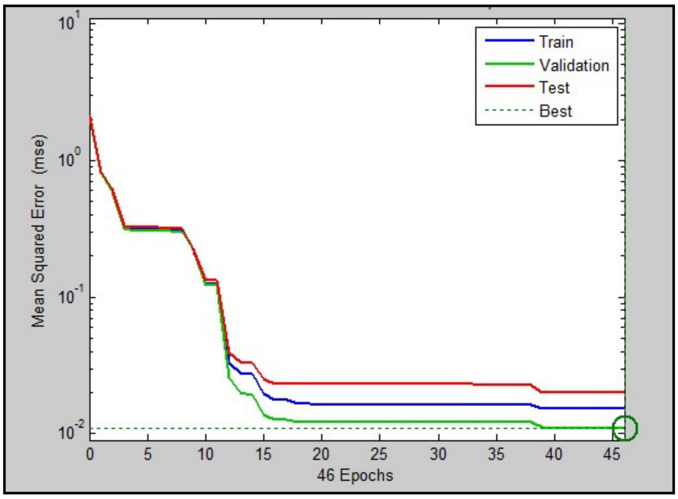


Figure 3.23 Training performance of ANN.

This work needs to explain the role of the IDS in the secure external communication for self-driving vehicles by calculating the performance metrics, as in the previous proposal. It is required to calculate PDR, throughput and average end-to-end delay for VANETs with IDS and infected VANETs with black hole attacks using Equations 3.8, 3.9 and 3.10. Table 3.20 shows the performance metrics for VANETs.

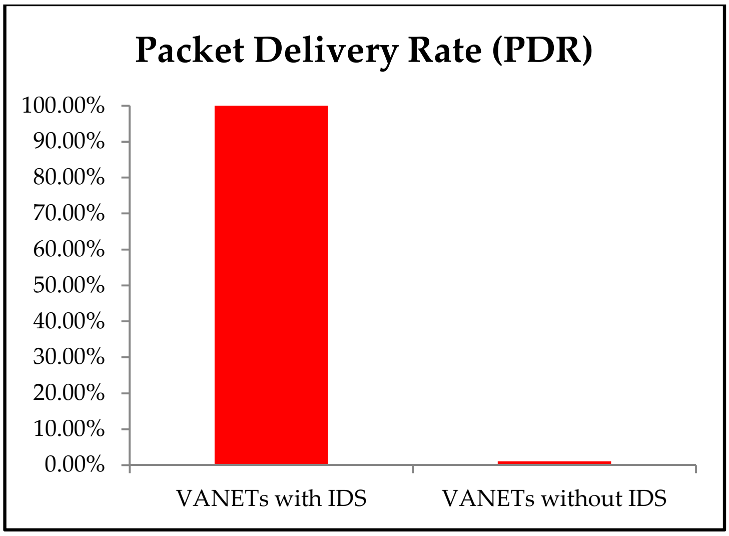


Figure 3.24 Packet Delivery Rate for VANETs.

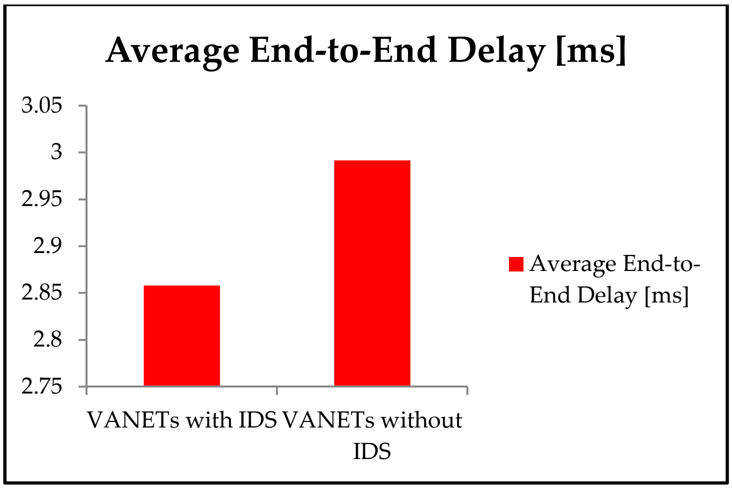


Figure 3.25 Average End-to-End Delay.

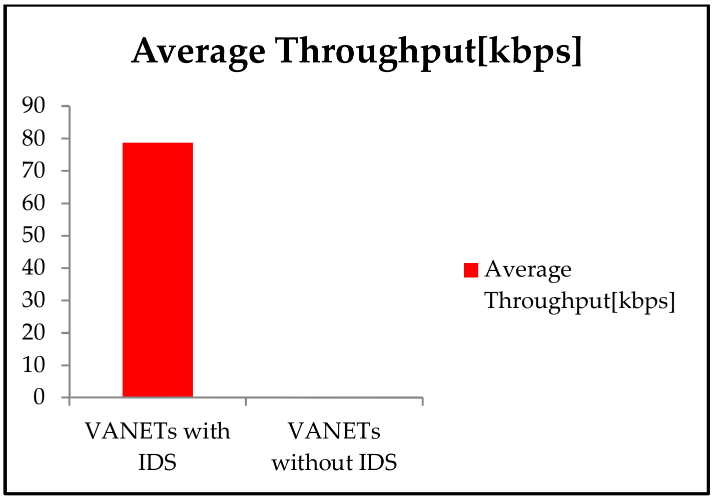


Figure 3.26 Average Throughput for VANETs.

Table 3.20 Performance Metrics for VANETs.

Performance Metrics	VANETs with IDS	VANETs Without IDS
Packet Delivery Rate	100.00%	1%
Average End-to-End Delay	2.858*ms*	2.9919*ms*
Average Throughput [kbps]	78.73	0.05

Figure 3.27 shows the performance metrics for VANETs with and without the IDS.

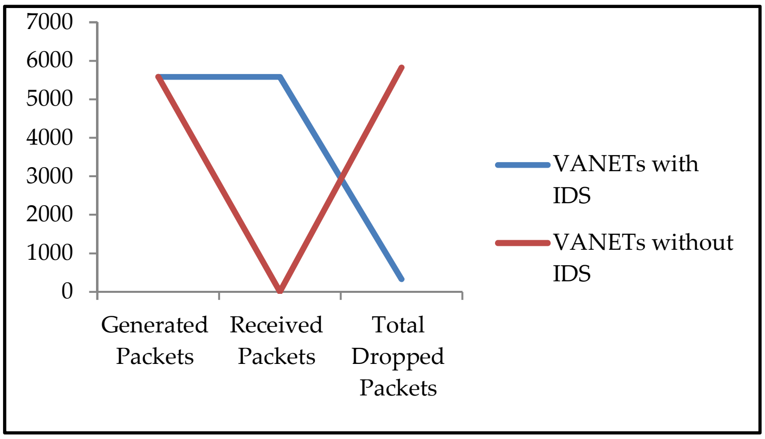


Figure 3.27 The Number of Sent, Received and Dropped Packets in VANETs.

3.3.1.1 Training and Testing the Neural Network (Misuse Detection Base)

The proposed IDS is trained and tested with the same fuzzification data in both phases (signature) to measure the accuracy of the detection rate and to calculate four types of alarm: true positive, false positive, true negative and false negative. Table 3.21 shows the detection rate accuracy and the number of records that were used in our proposed security system.

Table 3.21 Classification Rate of ANN and SVM.

IDS				
Class	**Original Records**	**SVM**	**Miss Records**	**Accuracy**
Normal	19329	19298	31	99.83%
Abnormal	10671	10654	17	99.84%
Class	**Original Records**	**FFNN**	**Miss Records**	**Accuracy**
Normal	19329	18973	356	99.15%
Abnormal	10671	10641	30	99.71%

Table 3.23 shows the rate of four alarms that were calculated by Equations 3.3, 3.4, 3.5 and 3.6 as shown in Table 3.22.

Table 3.22 Alarm Rates of ANN and SVM.

Alarm Type	FFNN	SVM
True Positive	99.96%	99.70 %
True Negative	99.91%	99.91 %
False Negative	0.03%	0.29 %
False Positive	0.08%	0.08 %

Figure 3.28 shows the performance comparison between the FFNN and SVM.

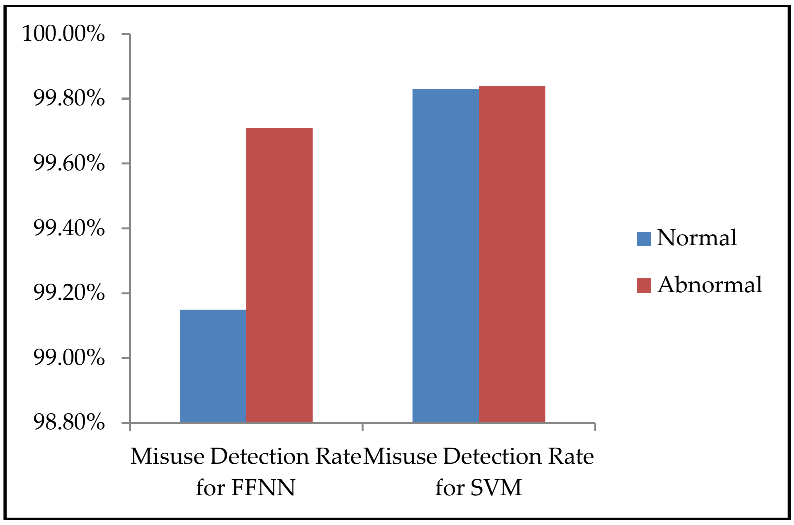


Figure 3.28 Performance Comparison between FFNN and SVM.

3.3.1.2 Training and Testing the Neural Network (Anomaly Detection)

The type and number of fuzzification that was utilised in the training phase differs from the data set that was used in the testing phase. The type of detection has the ability to detect novel or new attacks. Table 3.23 shows the accuracy of the detection rate and the number of records that were used in this proposed security system.

Table 3.23 Classification Rate of FFNN and SVM.

Intrusion Detection System				
Class	**Original Records**	**SVM**	**Miss Records**	**Accuracy**
Normal	25667	25612	55	99.78%
Abnormal	14333	14320	13	99.90%
Class	**Original Records**	**FFNN**	**Miss Records**	**Accuracy**
Normal	25667	25183	484	98.11%
Abnormal	14333	14300	33	99.76%

The rate of four alarms, time, error rate and Standard Deviation (SD) of FFNN and SVM that were calculated by Equations 3.3, 3.4, 3.5 and 3.6 are shown in Table 3.24.

Table 3.24 Performance Metrics of FFNN and SVM.

Alarm Type	FFNN	SVM
True positive	99.96%	99.61 %
True negative	99.88%	99.94 %
False negative	0.03%	0.38 %
False positive	0.11%	0.05 %
Time/s	0.99s	0.12s
Error Rate	0.15	0.21
Standard Deviation	0.102	0.429

In Table 3.24, time, error rate and SD are calculated to measure the efficiency of performance of FFNN and SVM as well as measure variation rate between them.

Figure 3.29 shows the performance comparison between the FFNN and SVM.

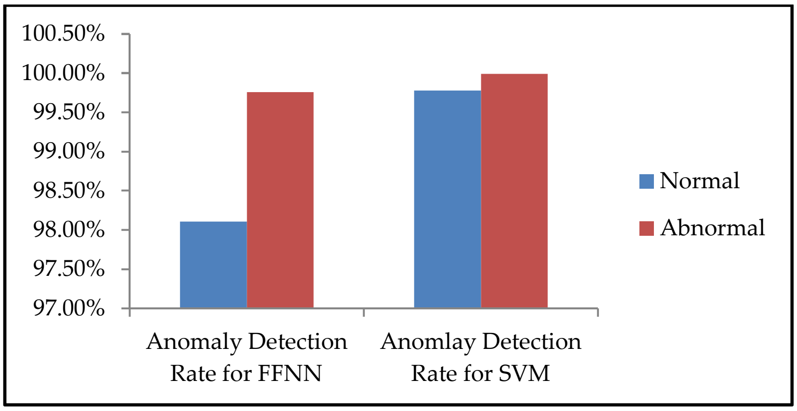


Figure 3.29 Performance Comparison between FFNN and SVM.

3.3.2 System Analysis

The methodology of the proposed security system was implemented in eight phases: generating the mobility and traffic model, the ns-2, the trace file, data collection and pre-processing, fuzzification data, training and testing for the FFNN, training and testing for the SVM and comparing the results that were generated in the two types of intelligent IDS.

When the two types of the proposed IDS are compared, the misuse IDS based on the SVM was more effective and efficient in detecting malicious vehicles with a lower false negative alarm rate as compared to the IDS based on the FFNN. SVM is faster than FFNN because the SVM automatically computes the number of hidden layers in an optimised way [168].

The error rate for the IDS based on the SVM was 0.16%. In this system, the alarm rate fluctuated between 99.91% and 99.61% with excellent and efficient accuracy. On the other hand, the false negative alarm rate was low in the anomaly detection system at about 0.38% which is a good indicator of the results.

Meanwhile, the error rate for the IDS based on the FFNN was 0.28%. The alarm rate fluctuated between 99.96% and 99.88% with good and efficient accuracy. On the other hand, the false negative alarm rate was low in the anomaly detection system at about 0.03% which is an excellent indicator of the results.

The detection rate is enhanced by using fuzzification data and two types of IDSs that create flexibility in selecting the system more efficiently with different conditions. In addition, in this proposal, the significant features were selected based on the previous study [160]. All these factors make the proposed security system more efficient in securing the external communication systems of self-driving and semi self-driving vehicles.

The proposed IDS was formally described in a research paper [169] which was presented at the 7th International conference in the School of Computer Science and Electronic Engineering (CEEC) - IEEE, University of Essex, 2015, Colchester United Kingdom, 2015.

3.4 Assessing the Proposed IDS with Kyoto Dataset

The proposed IDS, in this chapter, is tested with Kyoto dataset to evaluate the detection performance with a new dataset. Assessing the performance of the proposed IDS with a new dataset is important to check the efficiency of the security system. In addition, the role of the POS method and fuzzification model are distinguished in enhancing the detection rate and reducing the number of false alarms as well as improving consumer memory space and CPU speed. Figure 3.30 shows the basic architecture of the proposed IDS.

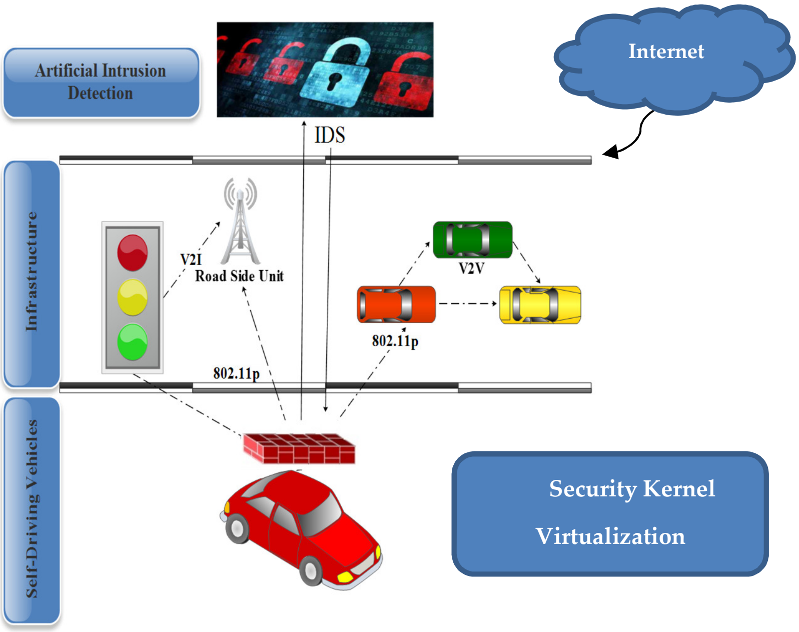


Figure 3.30 Network Architecture.

The proposed security system starts with collecting the behaviour of autonomous vehicles. The behaviours are analysed and then the IDS generates four types of alarms: True Positive, True Negative, False Positive and False Negative [170]. The steps below explain the Kyoto-IDS methodology and how we were able to reduce the number of Kyoto features and maintain the detection accuracy with fuzzification. Figure 3.31 shows the overall IDS architecture.

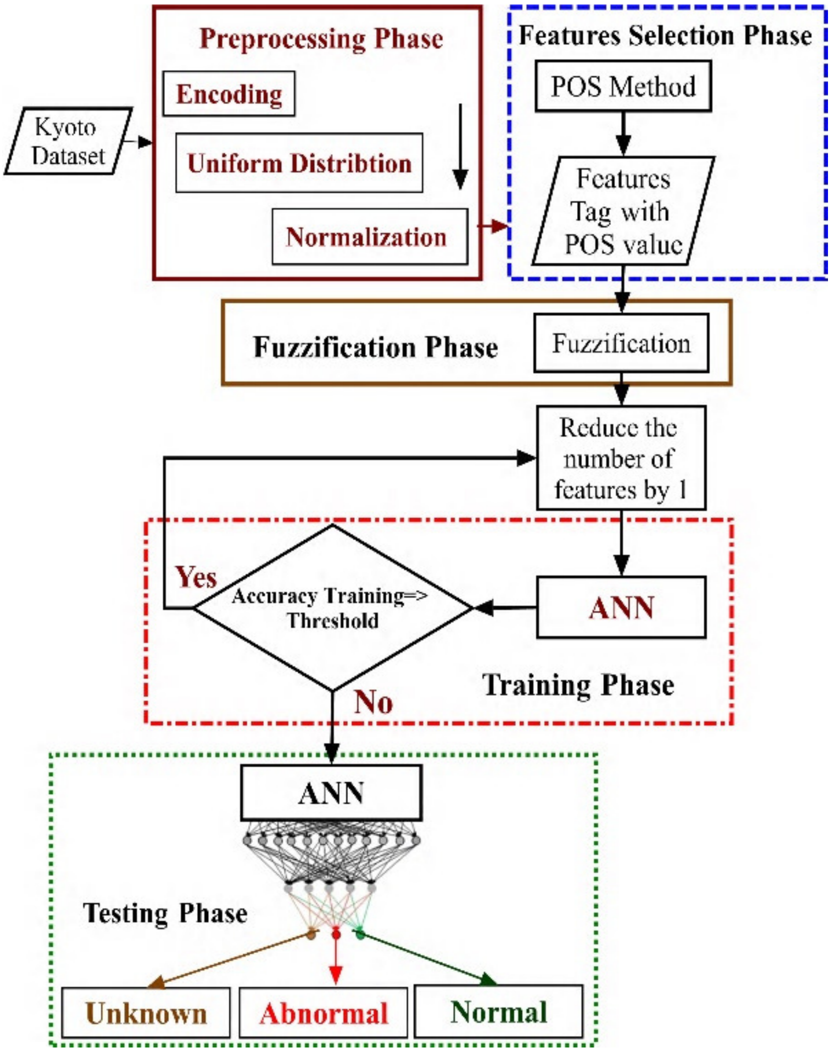


Figure 3.31 Overall IDS Architecture.

A. Benchmark Dataset Collection

One of the most important factor in evaluating the efficiency of the proposed IDS is dataset. Previous research mostly utilised KDD Cup99' for measuring the performance of security system [171]. Unfortunately, the proposed system cannot utilise KDD dataset for evaluating the performance of detection system because it suffers from a major problem of not covering current and recent network topology [172]. The intelligent IDS utilised Kyoto benchmark in testing performance of proposed security system. It is built from real traffic data on a network as well as honeypot dataset that was collected over three years. In other words, the Kyoto dataset is composed of:

- Kyoto data set with Internet Protocol (IP) source and IP destination.
- Kyoto data set without IP.

The dataset consists of 24 features that reflect normal and abnormal behaviour of nodes on network. Table 3.25 shows type of features:

Table 3.25 Features of Kyoto Data set.

Feature Name	Feature Source
Duration, Service, Source bytes, Destination bytes, Count, Same srv rate, Serror rate, Srv serror rate, Dst host count, Dst host srv count, Dst host same src port rate, Dst host serror rate, Dst host srv serror rate and Flag	KDD Cup 99’
IDS_detection, Malware_detection, Ashula_detction, Label, Source IP Address, Source Port Number, Destination IP Address, Destination Port Number, Start Time and Duration	Real Network

B. Extract the Impact of Features

In this subsection, the POS method and fuzzification model are approved in improving the detection rate, reducing the number of false alarms, enhancing consumer memory space and CPU speed. Table 3.26 shows the impact of the proposed Kyoto-IDS on the training time and memory consumption. Utilising 13 features reduces the time required by 11.4% and the memory required by 27.7%.

3.4 Assessing the Proposed IDS with Kyoto Dataset

Table 3.26 Metrics

Metrics	IDS with All Features	IDS with 13 Features
Memory Consumed	72e05b	52e05b
Time	24.31s	21.53s

In the training phase, the IDS can achieve 99.18% training accuracy with 13 features, that describe normal and abnormal behaviour in the Kyoto benchmark. Reducing the number of features is the fourth contribution of this chapter. The proposed Kyoto-IDS examined both all features and the 13 selected features. These features are shown in Table 3.27.

Table 3.27 Significant Features.

Significant Feature Name	Feature Source
Duration, Service, Source bytes, Destination bytes, Count, Dst host count, Dst host srv count, and Flag	KDD Cup 99'
Label, Source IP Address, Source Port Number, Destination IP Address, Destination Port Number and Duration	Real Network

The comparative evaluation results for different configurations of the IDS are shown in Table 3.28. The Kyoto-IDS is evaluated against a full set of features and then against a reduced set of features to establish the performance of the security system.

Table 3.28 Performance Metrics of ANN-IDS.

Metrics	IDS with all Features	IDS with 13 Features	IDS with 13 Fuzzification Features
Misuse Detection Normal	97.5%	99.79%	99.23%
Misuse Detection Abnormal	99.2%	64.34%	99.05%
Anomaly Detection Normal	92.04%	60.35%	99.04%
Anomaly Detection Abnormal	99.85%	98.45%	99.06%
Unknown Rate	28.5	0%	0.03
Average FP Alarm	2.27%	23.61%	1.82%
Average FN Alarm	1.01%	7.38%	0.4%

Average Error Rate	1.9%	19.32%	0.88%
Training Parameter Epochs	115	75	27

The vital role of the fuzzification dataset in enhancing detection rate, reducing the amount of false alarms and error rate as shown in Table 3.28. In addition, fuzzification features have a positive effect on time in the training phase for ANN by reducing the number of epochs.

3.4.1 Experimental Evaluation and Results

The proposed security system utilised a dataset of 40.000 records to reflect normal and malicious behaviour on network. The accuracy of detection rate in the training phase is 99.82% in this proposed IDS.

3.4.1.1 Training and Testing IDS with Misuse Detection

The proposed system is trained and tested with Kyoto dataset to evaluate its performance. The system calculated the classification rate and generated four types of alarms for the proposed IDS as shown in Table 3.29.

Table 3.29 Classification Rate of ANN-IDS.

Class	Original No.	Neural No.	Accuracy
Normal	3120	3042	97.5%
Abnormal	6873	6823	99.2%
Unknown	7	135	17.4%

Table 3.30 shows the rate of four alarms and error rate of detection system of communication of autonomous vehicles that were calculated based on Equations 3.3, 3.4, 3.5 and 3.6.

Table 3.30 Alarm and error rates of ANN-IDS.

Alarm	Rates
True positive	98.32%
True negative	98.90%
False negative	1.68%
False positive	1.1%
Error Rate	1.37%

3.4.1.2 Training and Testing IDS with Anomaly Detection

Misuse detection technique is utilised in this proposed IDS to detect and block internal and external attacks on the external communication system of self-driving vehicles. This detection system has two properties that made it more attractive in building IDS which are: a high detection rate and a low false alarm rate. Table 3.31 shows the detection rate and the number of records that were utilised in this proposed IDS.

Table 3.31 Classification rate of ANN-IDS.

Class	Original No.	Neural No.	Accuracy
Normal	3105	2868	92.04%
Abnormal	6890	7129	99.85%
Unknown	5	3	40%

Table 3.32 shows the alarm rate and error rate that were generated in this proposal based on Equations 3.3, 3.4, 3.5 and 3.6.

Table 3.32 Alarm and error rates of ANN-IDS.

Alarm	Rates
True positive	99.65%
True negative	96.54%
False negative	0.34%
False positive	3.45%
Error Rate	2.62%

The IDS was formally described in a research paper [173] that was presented at the 22nd IEEE International Conference on Automation and Computing (ICAC'16) - IEEE, University of Essex, 2016, Colchester, United Kingdom, 2016.

3.4.2 Assessing the Extracted Dataset with New IDS

The extracted dataset, in this chapter, is tested with new IDS to confirm the validity of the trace file that has been extracted from the ns-2. In other words, two IDS is proposed to prove that the extracted data is standard dataset for any IDS to evaluate the detection performance.

Discriminant techniques, whether linear or quadratic, are efficiently robust. Bayes optimal classifier is considered work principle of a discriminant methods as well the basic classification between classes in discriminant methods is based on a linear separating hyper plane is utilised in [174]. Table 3.33 shows classification rate of the proposed LDA and QDA that is based on trace file dataset.

Table 3.33 Classification Rate of LDA and QDA.

IDS			
Class	**Accuracy – Test Phase**	**Time/s**	**Error Rate – Train Phase**
LDA-Normal	99.94%	8.79	0.385%
QDA-Normal	81.09%		
Class	**Accuracy – Test Phase**	**Time/s**	**Error Rate – Train Phase**
LDA-Abnormal	91.07%	14.27	0.397%
QDA- Abnormal	78.87%		

In Table 3.34, four types of alarm are calculated for the proposed security system with new trace dataset.

Table 3.34 Alarm rates of LDA and QDA.

Alarm Type	LDA	QDA
True positive	86.44%	84.55%
True negative	92.73%	87.44%
False Positive	7.27%	12.56%
False negative	13.56%	15.45%

It is easily noticed that the LDA-IDS is more efficient and fast as compared to the QDA-IDS. In addition, the detection error rate of the LDA-IDS is less than that of the QDA-IDS. Hence, the IDS that is based on LDA is more efficient and effective in the detection of malicious behaviour for self-driving vehicles with a low false alarm rate as compared to QDA.

The IDS was formally described in a research paper [175] that was published in the Digital Communication and Networks– Elsevier Science Direct Journal, 2017.

3.4.3 System Analysis

Traditional security systems are not able to secure the VANETs of self-driving vehicles. In this case, these communication systems need to identify new protection methods or modify the current security schemes in order to establish efficient functionality in protecting the external communication system of vehicles.

Intelligent IDS can secure the external communication system of driverless vehicles by detecting and blocking malicious behaviour in its communication system. The proposed IDS in this chapter is mainly suitable for identifying malicious behaviour that targets vehicles disturbing the communication between self-driving vehicles. From experiment, an important role of the IDS is observed on the external security of communication vehicles under different condition.

When comparing these results with the previous paper [20], the proposed Kyoto-IDS can get a high detection rate with a low rate of false alarms in identifying abnormal behaviour of driverless vehicle.

In this proposed IDS, the alarm rate fluctuates between 92.4% and 99.85%; this enables an efficient detection rate with an average error rate of 3.30%, while the previous best achieved average error rate is 8.68% [20]. In [20], the average rate of false alarm is 4.86%, while we achieve 1.64% with the IDS presented here. Thus, experimental results confirm that the performance of Kyoto-IDS is efficient in detecting DoS of communicating self-driving vehicles.

3.5 Summary

An intelligent intrusion detection system is proposed in this chapter to secure the external communication system of self-driving and semi-autonomous vehicles. These security systems have been designed for training and testing of normal and malicious behaviours created on a simulator. They have to investigate and identify the behaviour of each self-driving vehicle to detect if it is a malicious vehicle or normal vehicle. One of the important properties for the proposed security system is the detection/stopping of both external and internal attacks.

Based on these experiments, the proposed hybrid IDS has demonstrated good detection rate with a low rate of false alarms. In addition, it plays an important role in blocking and identifying various attacks on the external communication systems. The process of decreasing the number of the extracted features by POS scheme has a vital role in enhancing the detection rate. In addition, the fuzzification on dataset helps reducing the error rate and the number of false alarms when compared with the previous studies.

3.5 Summary

The evaluation process of the proposed IDS with Kyoto benchmark dataset plays an important role in validating and measuring the efficient and effective detection performance in securing the external communication system of self-driving vehicles. This detection process and authentication technique of the security system are heavily based on novel features which are generated from different sensors of autonomous vehicles as will be illustrated in chapter four.

CHAPTER FOUR

AN INTRUSION DETECTION SCHEME FOR VEHICLES BASED ON ICMETRICS TECHNIQUE

"The most beautiful thing we can experience is the mysterious. It is the source of all true art and all science."

Albert Einstein

In this chapter, we propose that a novel IDS could protect these networks from any potential attacks that would have a direct and negative impact on the appearance of these self-driving vehicles. Recently, security in the majority of systems has been based on the concept of in-depth defense and specifically the use of multiple layers of defense to prevent adversaries from violating the security policies of these systems. IDSs can offer a second layer of defense for VANETs [176]. Figure 4.1 shows mobility vehicles, RSUs and the occurrence of an accident. Once an accident has occurred, CAMs and control data are created and communicated to the RSUs and other vehicles in that radio coverage area.

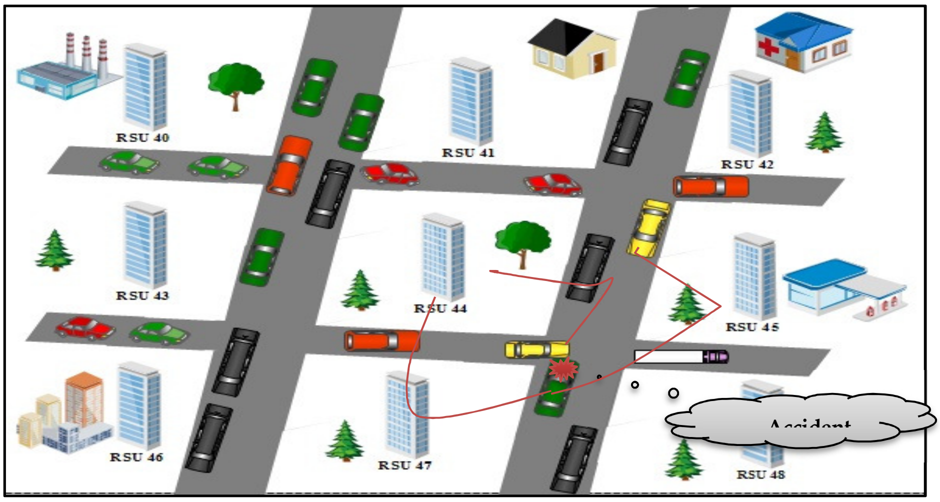


Figure 4.1 An Example of the Process of Responding to Cases of Emergency on the Road.

A novel IDS is proposed in this chapter to secure external communication system of self-driving and semi self-driving vehicles. It uses the latest ICMetrics technology to detect both internal and external attacks on external communication in self-driving vehicles. The ICMetrics technology uses internal features of a vehicle to generate an identification called an ICMetric. The ICMetric can be used to provide services related to authentication and attack detection. The ICMetric generation is an automated process and does not need user intervention. The ICMetric is generated when required and discarded there after thus reducing the chances of identity perversion.

Traditional IDS is combined with ICMetrics technology to achieve a robust security system of the external communication system of self-driving vehicles called ICMetric-IDS. Our research seeks to make two essential contributions in this chapter:

- Improving the authentication aspect of self-driving and semi self-driving vehicles by generating an ICMetric basis number, which was generated from bias reading of typical automotive sensors, such as accelerometer, gyroscope, magnetometer and ultrasonic sensors.
- Designing intelligent IDS based on the behaviour of self-driving or semi self-driving vehicles. These behaviours are identified as normal or abnormal which are extracted from the trace file. It was generated utilising ns-2 to model the VANET and its environment.

4.1 Self-Driving Vehicle Sensors

Self-driving and semi self-driving vehicles contain a huge number of sophisticated sensor devices that play a vital role in autonomous vehicles with different functions. These devices are frequently used to sense, predict and detect the status of the vehicle and its environment employing optical or electrical signals [147]. The sensors have the ability to generate signals from the physical characteristics they observe. They can be divided into three principle types: Micro Electro Mechanical Systems (MEMS), magnetic and light sensors [147].

The proposed security system presented here uses bias readings that have been extracted from sensor devices. These readings are used to generate ICMetric basis numbers that are employed as identification for self-driving vehicles. Recent research in the field of sensor-based identification has demonstrated that the use of sensory data is feasible and that it is possible to establish device identification [177], [178] and [179].

The main challenge is the design of the ICMetric basis number used for generating suitable features and identifying the sensor device's characteristics [180]. The suitable features must reflect the characteristics of the sensor devices; the extraction and the analysis process should not significantly influence the device performance. In this chapter, we get suitable features from the sensors to describe internal and external behaviour of vehicles, such as the ultrasonic crash sensor, gyroscopic, magnetometer and airbag accelerometers. The offset is utilised in the sensor measurement to our advantage and we propose a novel security system that generates an ICMetric basis number using the sensor bias readings.

4.1.1 Ultrasonic Crash Sensor

Autonomous and semi-autonomous vehicles are equipped with a sophisticated set of sensor devices that assist in providing various services required by the vehicles. These sensors have a substantial role in predicting the crash that helps the vehicles to introduce the safe mode at critical times. Every sensor has an offset that can be used to establish the identification of vehicles [135].

Self-driving vehicles utilise ultrasonic sensors for detecting the direction and calculating the distance of the object and pedestrian from time. In other words, the sound wave is taken to travel to object and back. In addition, these sensors have the ability to receive and emit ultrasonic that was a speaker or microphone. Table 4.1 shows the parameters of ultrasonic sensors that are utilised in proposed security system:

Table 4.1 Electric Parameters.

Parameters	Value
Voltage	DC 5 V
Current	15mA
Frequency	40Hz
Min & Max Range	2*cm* & 4*m*
Measuring Angle	15 degree
Echo output Signal	Input TTL level signal and the range proportion

The ultrasonic sensors in autonomous vehicles utilise sound propagation to identify pedestrian and object. In other words, these sensors use sonar to measure distances and detect stationary or moving objects in front or behind a vehicle up to a distance of four meters [181]; radar and sound navigation are used as acronym of term sonar. The ultrasonic sensor is also used to detect obstacles present in blind spots especially in intelligent parking assistance systems. The ultrasonic ranging Model HC-SR04 [181] sensor has been used to simulate the characteristics of a distance sensor in the design and implementation of the proposed security system. The ultrasonic sensor has an inherent bias which is unique to every sensor. This bias is utilised as a characteristic of the sensor to generate an ICMetric basis for the self-driving vehicle. Figure 4.2 shows the ultrasonic sensors in vehicles.

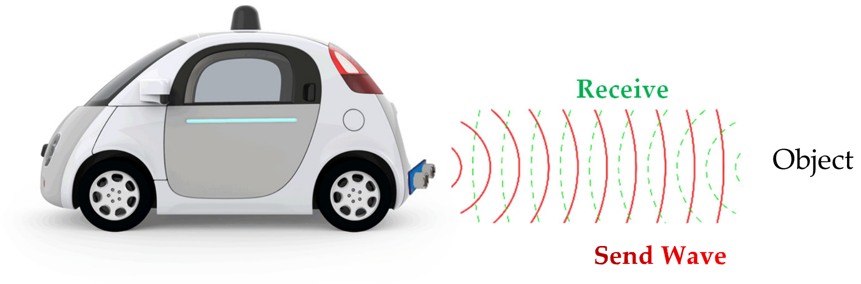


Figure 4.2 Ultrasonic Sensor.

4.1.2 Airbag Micro Electro Mechanical System Accelerometer

Micro Electro Mechanical System (MEMS) accelerometer is a technology that was first utilised in the automotive-airbag system in the 1990s [182]. This technology forms the design of a wide range of devices and systems in many industries [183], such as in automobile systems [184], mobile devices and structure monitors [185]. The MEMS accelerometer sensor is heavily employed in self-driving and semi self-driving vehicles [186]. A typical vehicle is embedded with three accelerometer sensors for airbag activation, active suspension control and for pedal position sensing. Figure 4.3 shows the accelerometer directions sensor in vehicles.

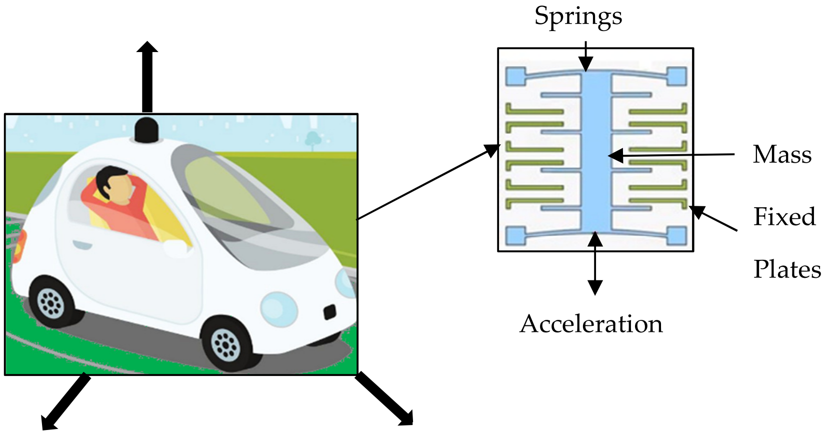


Figure 4.3 Accelerometer Sensor.

When an accelerometer sensor is embedded into a vehicle, it can be used to identify acceleration based unique behaviour of that particular vehicle. Owing to flaws in manufacturing, every MEMS based sensor has an inherent bias which is unique to the sensor. Owing to this bias, a sensor will generate a reading that differs slightly from the normal. Calibrations are introduced to correct this bias but still there is a residual error in the readings [135],[177],[178] and [187]. An output can be extracted when a static stimulus is applied to a MEMS and ultrasonic sensor device to generate ICMetric basis number. Table 4.2 shows some sensors and their offset that can be employed in identification of self-driving vehicles.

Table 4.2 Sensors and their Associated Bias.

Sensor	Imperfection
Ultrasonic	Linear bias
Accelerometer	Linear acceleration bias
Gyroscope	Linear gyroscopic bias
Magnetometer	Linear Magnetometer bias
Infrared	Nonlinear bias

4.1.3 Navigation Micro Electro Mechanical Systems Gyroscope Sensors

Self-driving vehicles, drones, digital camera, smart phones and stability controllers of vehicles are considered important applications of consumer electronics. These applications heavily depend on Micro Electron Mechanical Systems (MEMS) gyroscopes in their tasks [188]. The gyroscope sensors are categorised into three types: MEMS, optical fibre and ring laser [189]. This classification is based on work principle of this sensor. The performance and efficiency of optical fibre and ring laser gyroscopes in industrial machines are higher than MEMS. As we know, self-driving vehicles also require sensors have that high performance and efficiency. However, the cost and difficulty of application are big obstacles in designing navigation systems of self-driving vehicles with optical fibre and ring laser gyroscope [189].

Self-driving vehicles employ MEMS gyroscope to measure the angular rate that is based on Coriolis Effect as shown in Figure 4.4.

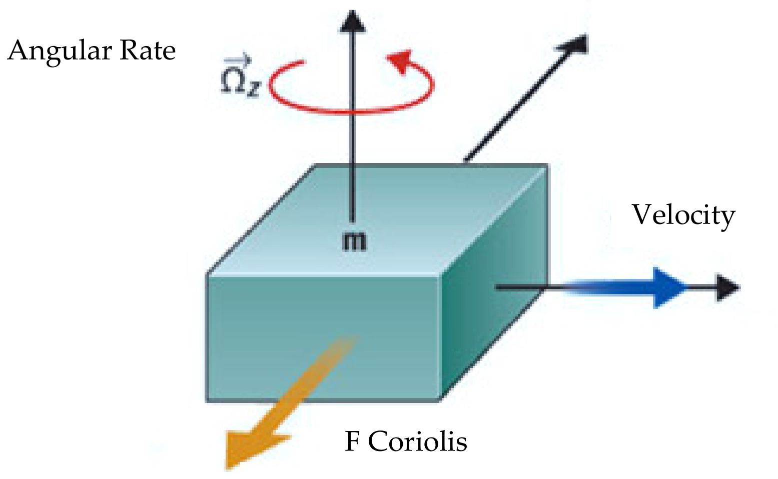


Figure 4.4 Gyroscope Sensor [190].

In Figure 4.4, mass (m) is passing in angular rotation velocity (*Ω*→) and directions (*v*→). However, drive axis and sense axis are represented by x-axis and y-axis respectively.

Employing MEMS gyroscope in the navigation systems can fix common problem of self-driving vehicles is GPS signals this event called "vehicle dead-reckoning backup system" [190]. In other words, the navigation systems of self-driving vehicles are based on yaw rate of gyroscope sensors to find the orientation to keep the vehicle moving on a digital map (e-maps) [190].

Bias readings stability that has been extracted from MEMS gyroscope are considered motivation to employ in designing a novel IDS. Moreover, the proposed ICMetric-IDS is based on individual characteristics of the manufacturing technology that was utilised in designing these sensors [135].

4.1.4 Micro Electro Mechanical Systems Magnetometer Sensors

Self-driving vehicles utilise MEMS magnetometer sensors for measuring and detecting magnetic fields. Hall Effect, Magneto-resistive effect and fluxgate effect are the most popular principles in magnetometer sensors [191]. Moreover, these sensors play important role in many applications, such as GPS navigation, magnetic field detection applications and electronic compass. In self-driving vehicles, the magnetic sensors have a number of applications, such as throttle, sunroof, wipers and wheel speed sensing. Self-driving vehicles employ MEMS magnetometer to measure the magnetic fields that is based on Hall Effect as shown in Figure 4.5.

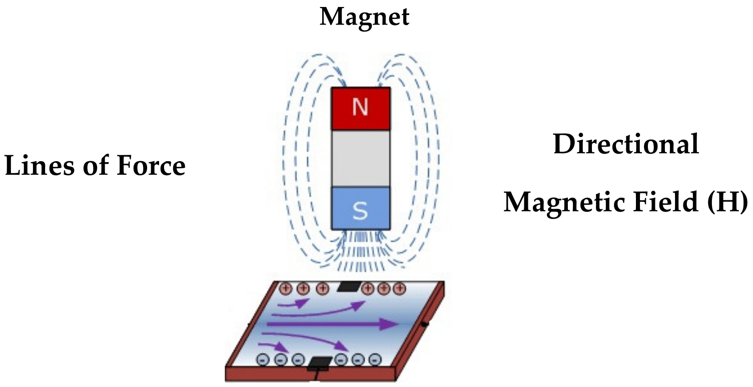


Figure 4.5 Magnetometer Sensor [192].

The proposed security system is dependent on unique features, which are extracted from bias readings of MEMS magnetometer sensors. These readings are considered novel features of magnetic sensors that are utilised in designing self-driving vehicles.

4.2 Integrated Circuit Metrics Technology

The key problem with existing security systems is that they are not sufficient for detecting the insider/internal attacks in wireless networks; they require additional security and defender systems like intelligent detection system to support their protection. The idea of the proposed IDS in this chapter depends significantly on potential features, which are generated from the characteristics of a specific embedded system [193]. These unique extracted features are called Integrated Circuit Metrics (ICMetrics). These features are viewed as a unique identifier for the specific system it is generated for.

4.2 Integrated Circuit Metrics Technology

ICMetrics is an emerging technology that uses features that have been extracted from the characteristics of an electronic system to form a unique identifier that can be used both for security and identification purposes, akin to the electronic equivalent of a biometric [193]. In this chapter, we are able to generate ICMetric basis number from bias readings that have been extracted from four types of sensors inside self-driving vehicles. The ICMetrics technology allows a device to generate an identity which is used for authentication, preventing identity misuse and a range of other cryptographic services.

The proposed IDS is based on an emerging protection approach called ICMetric technology. It is mainly based on inherent features that are extracted or derived from characteristics of sensors devices of self-driving and semi self-driving vehicles [193]. The generated features are considered a unique identifier that can be utilised to describe, detect or determine the vehicles. The main challenges in this domain are identifying the sensors devices' characteristics and extracting suitable features for the ICMetrics system [180]. In addition, the extracted features must reflect the characteristics of the sensor devices for vehicles, and the extracting and analysing processes of features should not significantly affect sensor device performance. Particularly, the suitable features are derived from bias readings of self-driving vehicles' sensors.

The type of extracted features is the main difference between the concept of ICMetrics technology and conventional traditional fingerprinting technologies [135]. Traditional hardware fingerprinting approaches are based on utilising inherent features which are static, easy to capture and use, such as CPU IDs, MAC addresses and serial numbers. The extracted features in traditional fingerprinting technologies are faced with many security problems, such as spoofed/replicated [135]. In addition, the fingerprinting technologies lack entropy and diversity because easily extractable for extracted features. Whereas extracted features in ICMetrics technology are difficult for an intruder to spoof/predict at runtime because ICMetrics utilises internal and various features to increase the complexity in the code breaking secret systems. In other words, it is employed application usage in selection of features such as browsing histories, system profile, camera resolutions, bias reading and GPS coordinates.

ICMetrics technology has demonstrated the ability to achieve a reliable authentication over traditional security systems that are based on password and identification numbers. It establishes the identity of a vehicle using their behavioural and physical characteristics. It has shown to be able to augment incumbent security technology in order to establish hardened protection [194]. The principle ICMetrics technology utilises two phases: the calibration phase and the operational phase [195].

The ICMetrics system requires these two phases to collect detailed knowledge or distribution of each extracted features for typical sensors.

4.2.1 Calibration Phase

The features and characteristics of a system are recorded and analysed in the calibration phase. In this phase, normalisation distributions are applied on feature values observed in the system. Statistical and mathematical operations on the extracted feature values are used to generate a device ICMetric basis number which uniquely identifies a device based on its low level features. Choice of features is an important factor because ICMetric is based on features which are unique and cannot be predicted or generated by an attacker. Finally, this calibration phase is applied once only when the system requires the ICMetric basis number.

4.2.2 Operational Phase

Following the calibration phase, the operational phase is then applied each time on the extracted features to generate a unique number. The extracted values are composed to form an ICMetric basis number in the operational phase. In this phase, the proposed security system applies the normalisation maps to generate unique features that distinguish it from others.

Figure 4.6 shows how the ICMetric basis number is generated by first applying the calibration phase. In this phase, the sensor readings are obtained following which they are subjected to statistical operations in the operation phase. In the operation phase an attempt is made to generate a resulting device ICMetric basis number through either feature concatenation or feature addition [193]:

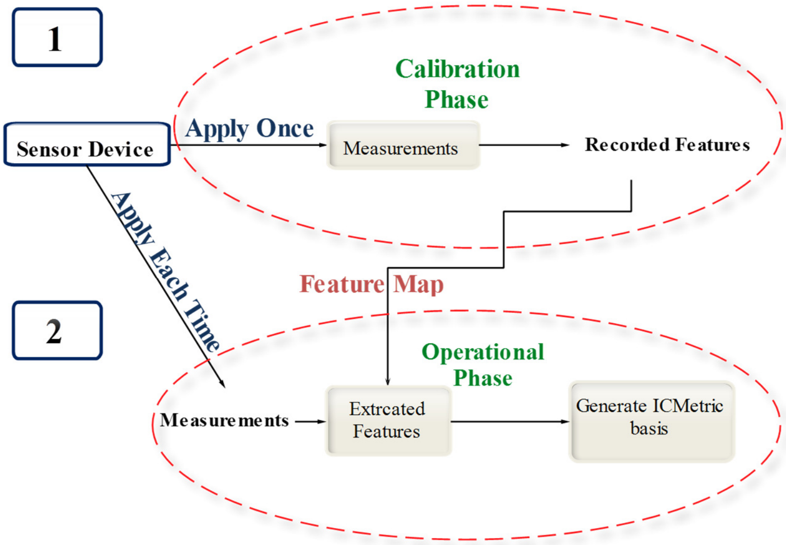


Figure 4.6 Process Flow Diagrams of ICMetrics Technology.

4.3 ICMetric-IDS Methodology

The proposed security system is composed of individual modules aimed at designing a security system based on the ICMetrics technology. We first collect bias readings from the ultrasonic, magnetometer, gyroscope and accelerometer sensors that are utilised in self-driving vehicles. The ICMetric basis number is generated from the bias readings obtained from the individual sensors. This is then studied in combination with a traffic and mobility scenario simulation. Malicious behaviour is simulated to determine how the system behaves when subjected to various forms of attacks. An ICMetric based trace file is generated and features are extracted to train the FFNN and k-NN. The POS method that was mentioned in Chapter three is used to extract significant features from a wider range of features available in the trace file. Feature values are fuzzified and the intelligent detection system is trained and tested to detect intrusions.

4.3.1 Sensor-Based Offset Measurement

Sensor-based offset cannot be obtained for every sensor. In some cases, it is infeasible to collect the bias in the sensor. The offsets of sensors are extracted and normalised to determine if they are truly unique and deterministic. For generating the bias readings of a system, those sensors are required which are not affected by external factors and also do not require user intervention. For instance, the engine temperature sensor cannot be used since it is subjected to varying weather conditions. Other sensors, like the oxygen sensor, cannot be used as the amount of oxygen varies in the atmosphere with change in altitude [196]. Our proposed system uses the ultrasonic and MEMS sensors because they are readily available and also because the required stimulus is easy to create.

4.3.1.1 Ultrasonic Sensors

The ultrasonic sensor is a distance measuring sensor designed to measure distances between vehicles and objects, and alert early for any expected accidents. It is composed of ultrasonic transmitters, receiver and control circuit [197]. The ultrasonic sensor must be placed on a stable place that is free from erratic movements to extract the offset values [135]. Using the ranging Model HC-SR04 sensor as an experimental platform, we obtained 4500 individual readings from the ultrasonic sensor. These sensor devices are embedded in the ultrasonic transmitter and receiver module. The output readings from the sensors are saved in a CSV file at regular intervals. Three ultrasonic sensors are utilised to prove that each sensor behaves differently when subjected to the same stimulus. The raspberry pi is used as an embedded platform and use the sensors to create a system prototype as shown in Figure 4.7.

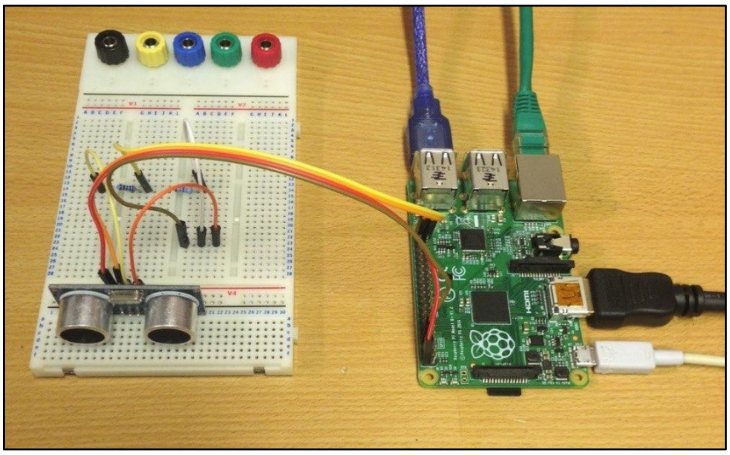


Figure 4.7 An Ultrasonic Sensor with Raspberry pi used to determine the Ultrasonic Bias.

The number of readings influences the stability of the ICMetric basis number. A large number of readings ensures that sufficient population representation is used in the statistical analysis. If the number of readings is too small, then the resulting statistical analysis will be flawed as this does not completely represent the full population. Figure 4.8 shows a graph in which the convergence of sample means and population mean has been depicted. As the number of readings increases the two mean values converge to a single reading. While generating the ICMetric, the point of convergence needs to be determined which in our case is 4500 readings from the ultrasonic sensor.

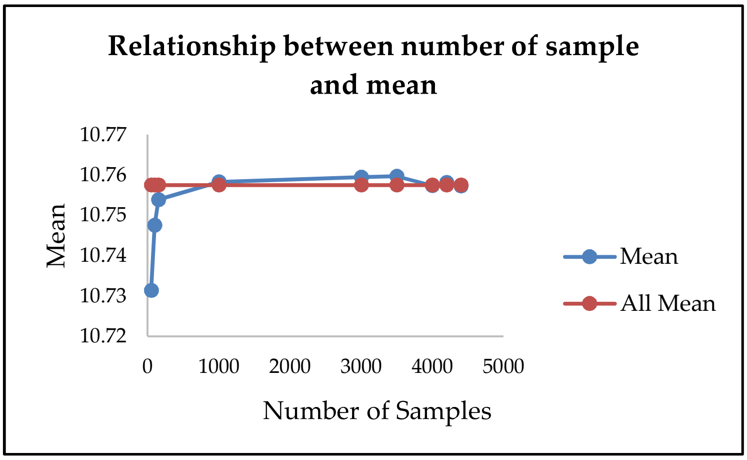


Figure 4.8 The Relationship between Sample mean and Population Mean.

Figure 4.9 shows that each sensor possesses a bias which is unique to the sensor. This ultrasonic proves that the extracted reading can be used for the establishment of an ICMetrics basis number. The unimodal distribution for the three sensors is shown in Figure 4.9.

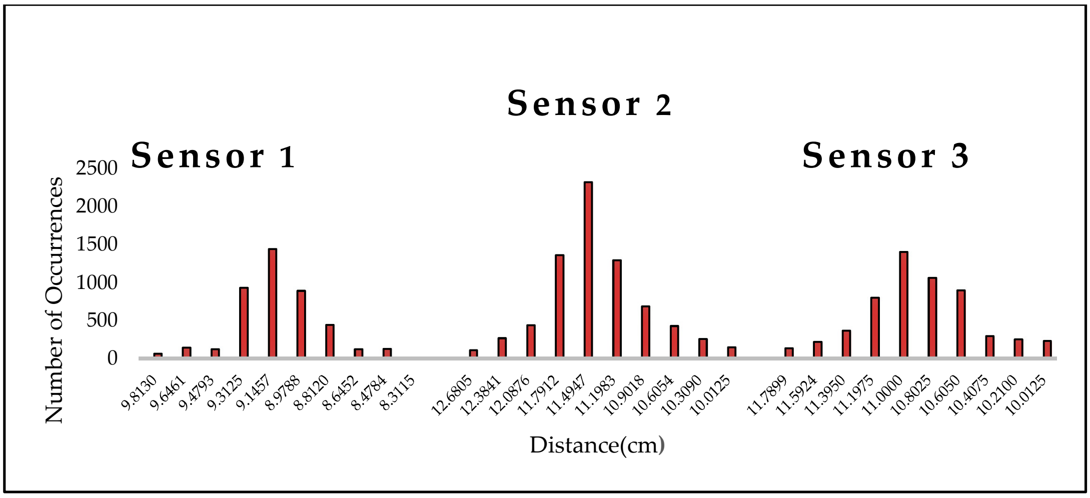


Figure 4.9 Calibrated Ultrasonic Unimodal Distribution Graphs for three different Sensors.

4.3.1.2 Micro Electro Mechanical Systems Sensor

In the proposed security system, myAHRS_plus sensor is utilised in designing IDS that is considered one of the most accurate sensors in the scientific research area [198]. It is an embedded sensor triple axis accelerometer with a sensitivity of ±16g and consists of also a gyroscope and a magnetometer sensor that are shown in Figure 4.10.

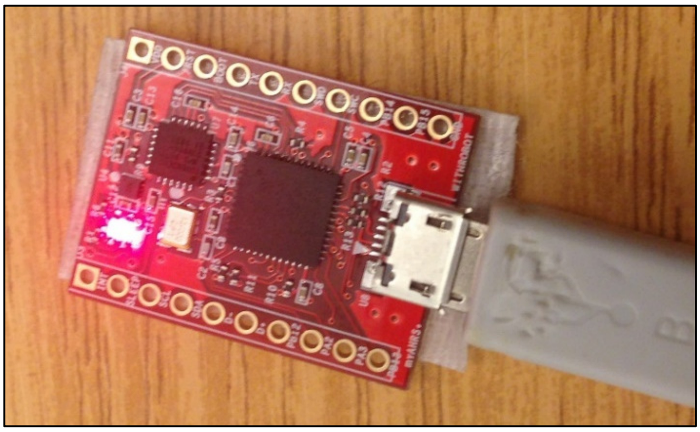


Figure 4.10 myAHRS_plus Sensor.

Different number of bias reading are extracted from myAHRS+ to generate ICMetric basis number. In this case, the security system needs scientific justification to determine the optimal number of offset readings that are used in designing the IDS. The number of bias readings influences the stability of the statistical processes of the ICMetric generation. To determine the optimal number of readings, we need to calculate the population mean and compare the result with the mean value calculated for a smaller subset of readings. The MEMS demonstrated that lesser number of readings are required to achieve a mean convergence point. The optimal number is 950 but we used 1000 bias readings to obtain a more accurate system that is shown in Figure 4.11.

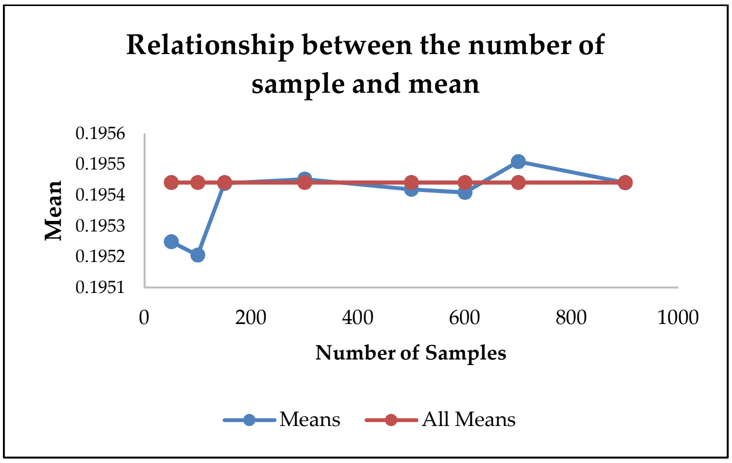


Figure 4.11 The Relationship between Population Mean and Sample Mean.

The offset readings obtained from the x, y and z axis of the MEMS sensor make it a suitable candidate for the generation of a device ICMetric. The calibration matrices in our research are generated for x, y and z axis of three types of MEMS sensors. Figure 4.12 (a) shows the unimodal distribution for the three axes of a single accelerometer sensor based on our measurements.

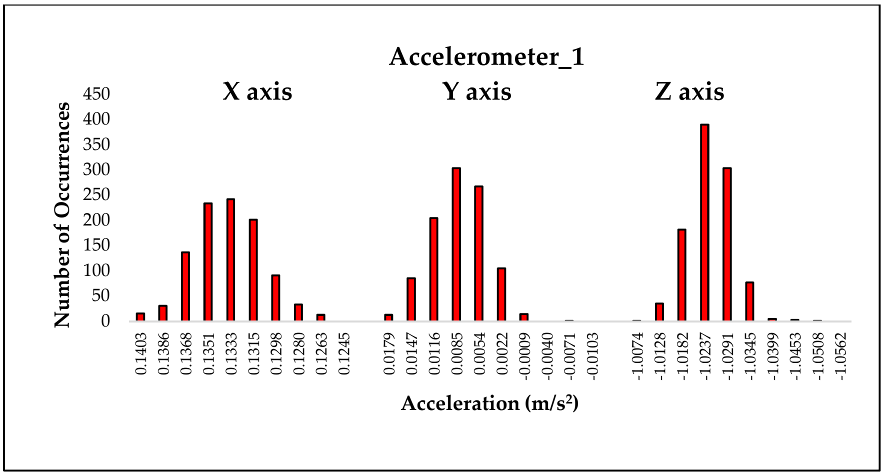


Figure 4.12 (a) Calibrated Normalisation Map for the three Axes of a Single Accelerometer Sensor.

In addition, the measured characteristics for the triple axis of two accelerometer sensors are shown in Figure 4.12 (b).

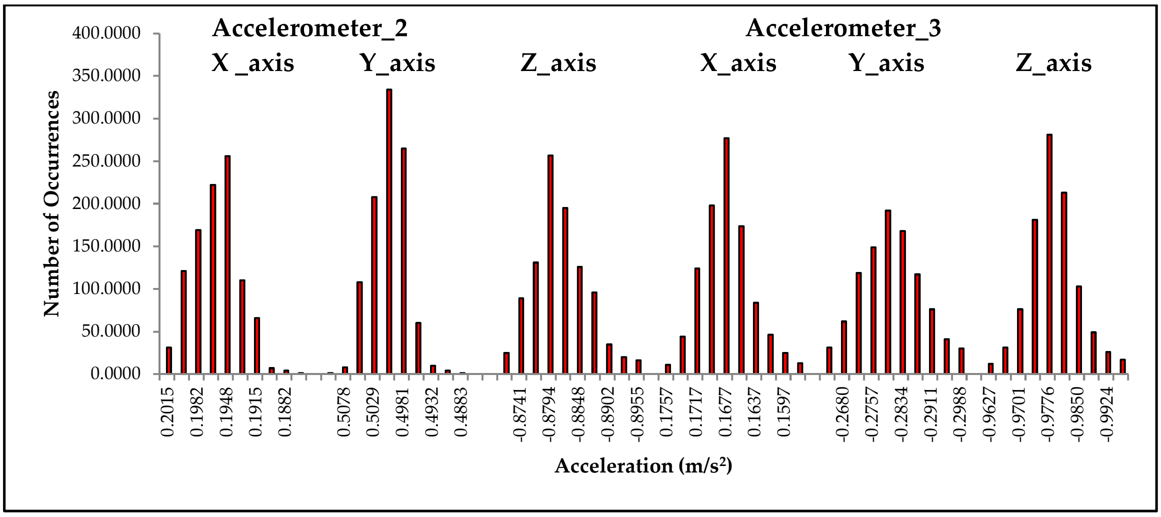


Figure 4.12 (b) Calibrated Normalisation Map for three axes of two Accelerometer Sensors.

Figure 4.13 (a) and (b) show bias readings that are generated from gyroscope sensors. In this proposed security system, three gyroscope sensors are employed to establish ICMetric basis number to protect the external communication system from possible attacks.

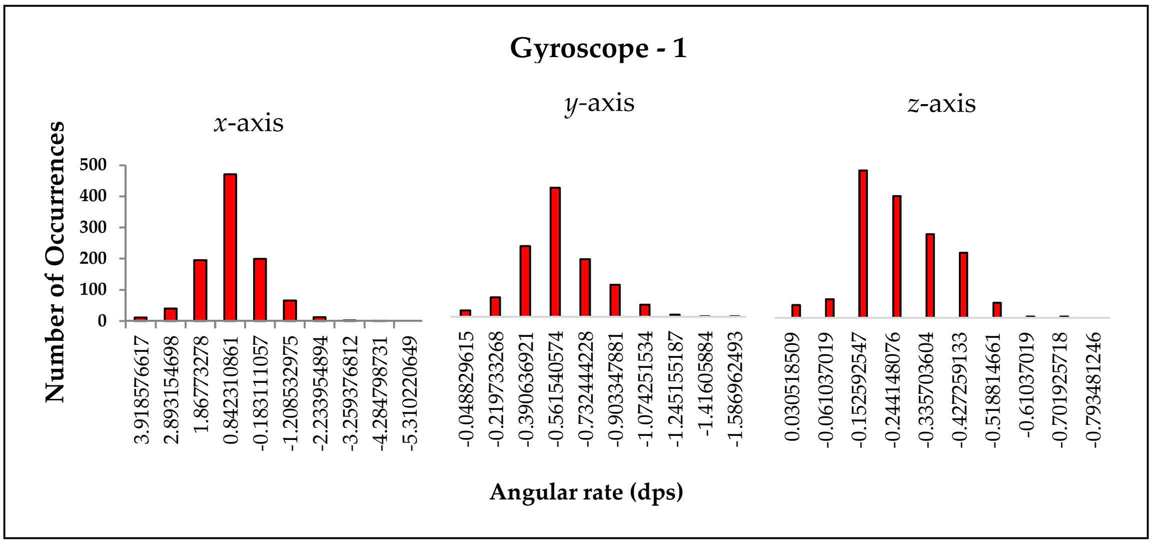


Figure 4.13 (a) Calibrated Normalisation Map for three Axes of a Single Gyroscope Sensor.

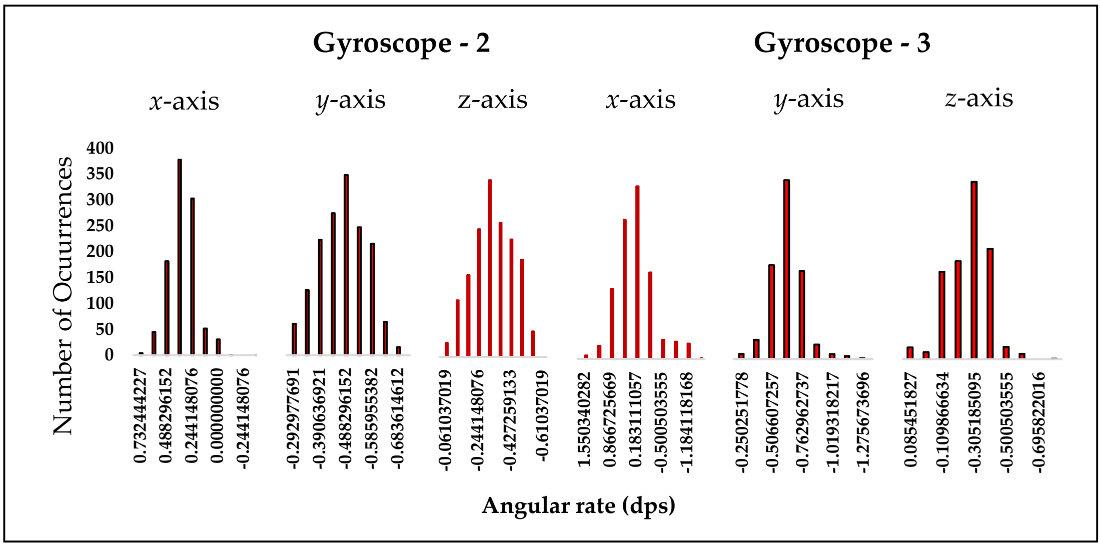


Figure 4.13 (b) Calibrated Normalisation Map for three Axes of Two Gyroscope Sensors.

Whereas the bias readings of three magnetometer sensors are shown in Figure 4.14 (a) and (b).

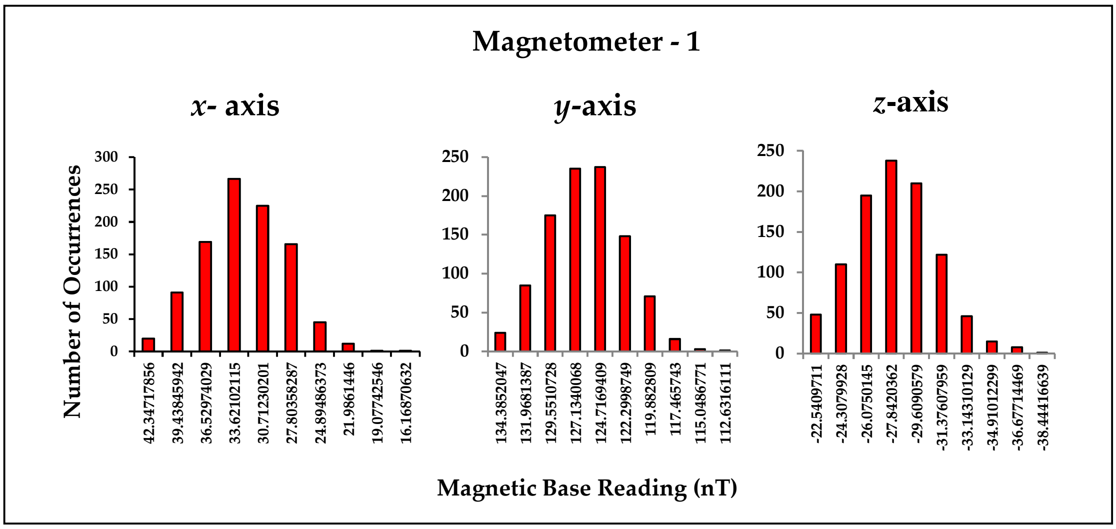


Figure 4.14 (a) Calibrated Normalisation Map for the three Axes of a Single Magnetometer Sensor.

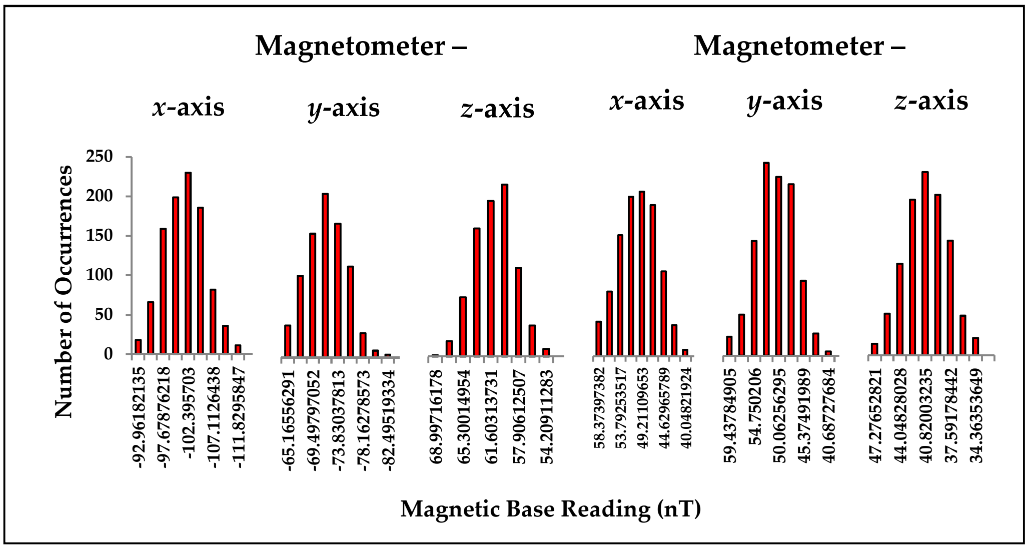


Figure 4.14 (b) Calibrated Normalisation Map for three Axes of two Magnetometer Sensors.

4.3.2 Statistical Analysis for ICMetrics

Statistical functions are utilised to study features for ICMetric basis number generation [199]. Sensor readings are obtained from ultrasonic, accelerometer, gyroscope, infrared and magnetometer. In other words, the generating process needs a probability mass (x) function to determine the precise value from the bias reading [199]. A Probability Mass Function (PMF) is a statistical probability function that is employed to calculate the probability of bias readings from various sensors. Hence, probabilities are calculated through bias readings through PMF [200]. The bias readings that are generated from sensors that have a defined a real valued function. In other words, this numerical valued function is a random variable [201]. These variables are classified into two types which are discrete and continuous [201]. The discrete random variable can take a countable infinite value number. However, discrete random variables are associated with the outcomes of random bias readings of sensors. Specifically [201], the bias reading in sensors provides a discrete random variable which can take on a set of possible readings. When eliminating outliers, it is evident that data is discrete random variable. The PMF is given by Equation (4.1), if (σ^2) is the SD.

$$p(x) = \frac{1}{\sigma\sqrt{2n}}\, e^{\frac{-(x-\mu)^2}{2\,\sigma^2}} \tag{4.1}$$

According to Equation (4.1), the probability mass (x) function is composed of other statistical function that is identified for generating the ICMetric basis number. In addition, the mean ($\bar{X}$) and standard deviation (σ^2) are calculated to determine the (x) value. Equation (4.2) is used to calculate the mean:

$$\bar{X} = \frac{1}{n} \sum_{i=1}^{n} x_i \tag{4.2}$$

where x is an individual ultrasonic, accelerometer, gyroscope and magnetometer reading and n is the total number of bias data obtained from the sensors. Equation (4.3) is used to calculate the standard deviation (σ^2):

$$\sigma^2 = \sum_{i=1}^{n} p(x_i)\,(x_i - \bar{X})^2 \tag{4.3}$$

In addition, other statistical and mathematical functions are employed to analyse the generated reading, such as:

- Confidence Interval (CI) is used to estimate the range being calculated from the offset readings:

Upper and Lower bound of CI = $\bar{x} \pm z\frac{\sigma}{\sqrt{n}}$ (4.4)

where, z= 1.96 for a 95% confidence interval [202].

- Inter Quartile Range (IQR) is the difference between the third and the first quartile in offset data. It is a calculation of how spread out the bias readings are around the mean:

$$IQR = Q_3 - Q_1 \tag{4.5}$$

where, Q_3 and Q_1 are the upper and lower quartile respectively.

- The Variance (s^2) is a measure of dispersion for extracting readings:

$$s^2 = \frac{1}{n-1}\sum_{i=1}^{n}(x_{\mathrm{i}} - \bar{x})^2 \tag{4.6}$$

where, n is the total number of bias data obtained from the sensors and x-bar is the mean.

- The Skewness distribution (S) is a measure of asymmetry of the probability distribution of bias readings; it can be negative or positive:

$$S = \frac{3(\bar{x} - mdian)}{\sigma^2} \tag{4.7}$$

- The P-value is a statistical indicator which shows that there is sufficient statistical difference between the readings. It forms the basis for the acceptance or rejection of the null hypothesis [203]. The P-value ranges from 0 to 1 where 0 means no similarity between the readings while 1 means high certainty of similarity.

Some statistical and mathematical functions are applied in Table 4.3 that were earlier used to calculate the metrics for the graphs in Figures 4.9, 4.12, 4.13 and 4.14.

Table 4.3 Statistical Analysis of the Unimodal Distribution for the Ultrasonic, Accelerometer, Gyroscope and Magnetometer Devices.

Statistical Functions	Sensor_1	Sensor_2	Sensor_3
Confidence Interval	(9.0422, 9.0274)	(11.0833, 11.0624)	(10.8294, 10.8169)
Standard Dev.	0.2492	0.4548	0.2433
Inter Quartile range (IQR)	0.2575	0.7523	0.2248
Mean	9.0369	11.0789	10.8250
Skewness	0.0138	0.8155	0.9650
Variance	0.0621	0.2068	0.0591

P-value	0.00

Statistical analysis of x, y and z axis in three different Accelerometer, Gyroscope and Magnetometer Devices

Statistical Functions	Accelerometer_1		
	X-axis	Y-axis	Z-axis
Confidence Interval	(0.1327, 0.1324)	(0.0069, 0.0064)	(-1.0272, -1.0279)
Standard Dev.	0.00268	0.0037	0.0053
Inter Quartile Range (IQR)	0.00341	0.0053	0.0068
Mean	0.1326	0.0066	-1.0275
Skewness	-0.0349	0.1152	-0.0610
Variance	7.21091E-06	1.43403E-05	2.82819E-05
P-value		0.00	

Statistical Functions	Accelerometer_2		
	X-axis	Y-axis	Z-axis
Confidence Interval	(0.1956, 0.1952)	(0.4996, 0.4992)	(-0.0881, -0.8822)
Standard Dev.	0.00264	0.0028	0.0044
Inter Quartile Range (IQR)	0.00342	0.0039	0.0058
Mean	0.1954	0.4994	-0.8819
Skewness	-0.01518	-0.0986	0.0871
Variance	7.00621E-06	8.07228E-06	1.94442E-05
P-value		0.00	

Statistical Functions	Accelerometer_3		
	X-axis	Y-axis	Z-axis
Confidence Interval	(0.1674, 0.1671)	(-0.2794, -0.2803)	(-0.979, -0.9803)
Standard Dev.	0.0028	0.0071	0.0042
Inter Quartile Range (IQR)	0.0034	0.0185	0.0063
Mean	0.1673	-0.2798	-0.9800
Skewness	0.0095	0.1730	0.1486
Variance	8.09261E-06	5.14123E-05	2.36604E-05
P-value		0.00	

Statistical Functions	Gyroscope_1		
	X-axis	Y-axis	Z-axis

Confidence Interval	(0.3205, 0.1867)	(-0.6656, -6.922)	(-0.2954, 0.3098)
Standard Dev.	1.0795	0.2151	0.1171
Inter Quartile Range (IQR)	1.1291	0.2441	0.1221
Mean	0.2536	-0.6789	-0.3024
Skewness	-0.0175	-0.0878	0.0281
Variance	1.1652	0.0463	0.0137
P-value		4.7557E-202	

Statistical Functions		**Gyroscope_2**	
	X-axis	**Y-axis**	**Z-axis**
Confidence Interval	(0.2425, 0.2582)	(-0.5022, -0.5127)	(-0.3312, -0.0053)
Standard Dev.	0.126844115	0.0852	0.086142153
Inter Quartile Range (IQR)	0.122074038	0.1221	0.061037019
Mean	0.250434889	-0.5075	-0.336558123
Skewness	0.270088788	0.0891	0.169868043
Variance	0.016089429	0.0073	0.00742047
P-value		0.00	

Statistical Functions		**Gyroscope_3**	
	X-axis	**Y-axis**	**Z-axis**
Confidence Interval	(0.2962, 0.2577)	(-0.6910, -0.7080)	(-0.3003, -0.3158)
Standard Dev.	0.3109	0.1373	0.1247
Inter Quartile Range (IQR)	0.3662	0.1831	0.1831
Mean	0.2769	-0.6995	-0.3081
Skewness	0.2910	-0.2828	0.0926
Variance	0.0967	0.0188	0.0155
P-value		0.00	

Statistical Functions		**Magnetometer_1**	
	X-axis	**Y-axis**	**Z-axis**
Confidence Interval	(31.4568,30.9338)	(125.1675, 124.6984)	(-28.7284, -29.0831)
Standard Dev.	4.218985944	3.784291053	2.860914541
Inter Quartile Range (IQR)	5.90990936	5.1454207	3.9208655
Mean	31.19535813	124.9330027	-28.90580157
Skewness	-0.000881593	-0.003934633	-0.180903772
Variance	17.79984239	14.32085877	8.18483201
P-value		0.00	

Statistical Functions	**Magnetometer_2**		

	X-axis	Y-axis	Z-axis
Confidence Interval	(-102.5211, -103.0188)	(-72.5730, -73.0026)	(60.3743, 60.0407)
Standard Dev.	4.015104407	3.466054182	2.690850552
Inter Quartile Range (IQR)	5.706198312	4.94399854	3.68968779
Mean	-102.7699637	-72.78785363	60.20756554
Skewness	0.065459667	-0.016225336	0.04191755
Variance	16.1210634	12.01353159	7.240676692
P-value	0.00		
Statistical Functions	Magnetometer_3		
	X-axis	Y-axis	Z-axis
Confidence Interval	(49.2086, 48.7042)	(49.7952, 49.3480)	(40.0403, 39.7036)
Standard Dev.	4.068817756	3.606942915	2.715888261
Inter Quartile Range (IQR)	5.74053164	5.00808741	3.78124332
Mean	48.95645314	49.57165136	39.87197485
Skewness	0.135312932	0.083964566	0.106800676
Variance	16.55527793	13.01003719	7.376049045
P-value	0.00		

The most important attribute of this technology is that the ICMetric basis number is not transmitted between vehicles and their RSUs, and also not stored in the system protected by this technology. The ICMetric basis number is utilised as a feature which can be incorporated into the trace file. Since the ICMetric is not stored in its raw form, therefore, any attack on the trace file does not expose the ICMetric stored on the file.

This characteristic has made systems that rely on ICMetrics technique for protection more exciting and attractive in the scientific research area. Figure 4.15 shows the elapsed time in second (*s*) to analyse readings for generating the ICMetric value with different number of ultrasonic crash sensors, accelerometer, gyroscope and magnetometer sensors.

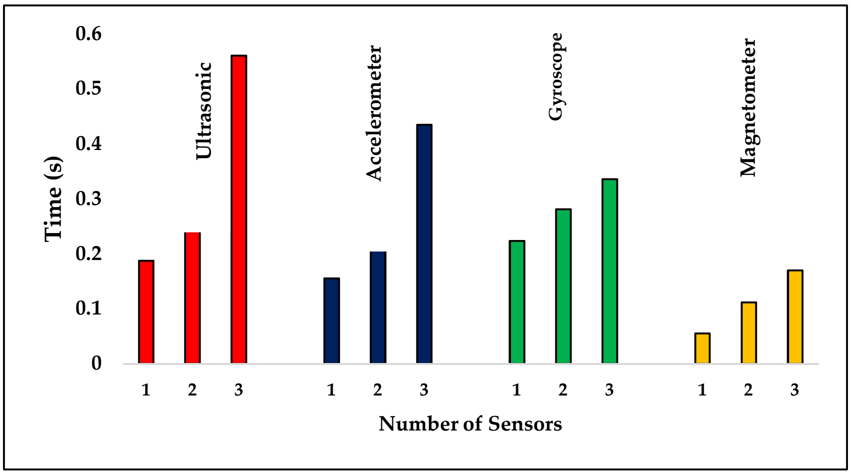


Figure 4.15 The Elapsed Time of Sensors.

4.3.3 Simulation System

a. Simulation of Traffic and Mobility Scenarios

Two softwares are utilised to generate a real-world traffic of abnormal/ normal behaviour for self-driving and semi self-driving vehicles. These tools are: SUMO and MOVE [98]. The output files of these tools are used as input for ns-2 [151]. The reasons for employing the SUMO to generate mobility scenario are: open source, widely used in VANETs, microscopic and multi-model traffic simulation [87]. In addition, it is computationally efficient and easily adapts with various number of vehicles as well as the MOVE model designed on SUMO [204], [205] with Java interfaces.

The mobility models are divided into three types: urban, highway and rural model [156]. The urban mobility model includes many kinds of model, such as Random Way Point (RWM) model, Manhattan mobility model and Rice University Model (RUM) [156]. In this chapter, the Manhattan mobility model is used in designing mobility environment because it is widely used in the research field and it allows vehicles to move in different directions – vertical and horizontal [156].

b. Simulation Parameters and Environment

To test the design of the proposed system, it was implemented on an Intel 5744 Core i3-380M processor running at 2.53 GHz with 4GB RAM. To prove the efficiency of the schemes, simulation was carried out in MATLAB. The cryptographic module was designed in Dev-C with OpenSSL providing the cryptographic libraries. The system was designed with a 128-bit random salt value that works with an assumed ICMetric basis. The simulation of Urban Mobility Model and MObilty VEhicles are integrated with ns-2 to generate the normal and malicious behaviours.

The simulation process is conducted with the ns-2.35RC7 environment on a platform and Ubuntu 14.04 LTS to evaluate and measure the performance of the proposed IDS. It is designed to simulate various networks, such as wireless and wired networks [98]. The simulator has many characteristics that have encouraged many researchers to use it, such as open source, low cost, fast and a rich library. Moreover, it has the ability to adapt to different networks and speed of simulation [151].

The external communication system of self-driving vehicles is created on the ns-2 to simulate the proposed security system. We face problem in simulating the communication system for autonomous systems with ns-2 because it is not designed specifically for VANETs. For this purpose, extra software is employed for the VANETs simulation: SUMO and MOVE or CityMob [50]. The mobility system uses the ns-2 to achieve the intelligent IDS for the external communication of autonomous vehicles in real-world. The ns-2 generates two output files: trace file and Network Animator (NAM) that describe the external behaviour of vehicles [98].

The proposed system is based on features that were extracted from the ns-2 trace file of routing protocol. The system processes the features from the trace file of routing protocol. Hence the system can be adapted to any routing protocol.

4.3.3 Simulation System

The initial parameters are one of the important issues in ns-2 because they play a vital role in specifying the performance, mobility, traffic type and behaviour of vehicles. In Table 4.4, some parameters used in simulating VANETs are given. Constant Bit Rate (CBR) application that sends constant packets through a transport protocol, such as (UDP or TCP), and Radio Propagation Model (Two Ray Ground) [98].

Table 4.4 Simulator Environmental and Parameters.

Parameter	Value
Simulator	ns-2.35
Simulation time	499*s*
Number of nodes	150 Vehicles
Number of RSUs	12 RSUs
Type of Traffic	Constant Bit Rate (CBR)
Topology	600 x 600 (*m*)
Transport Protocol	UDP- TCP
Packet Size	512
Routing Protocol	V-AODV
Channel type	Wireless
Queue Length	50 packets
Number of Road Lanes	4
Radio Propagation Model	Two Ray Ground
MAC protocol	IEEE 802.11p
Speed	40 m/s
Interface queue type	Priority Queue
Network Interface type	Physical Wireless
Mobility Models	Manhattan Mobility Model

c. Generating Malicious Behaviour

In this chapter, we need to modify and add some files to the routing protocol to generate the malicious behaviour in external communication of driverless vehicles to evaluate and measure the performance of the proposed IDS. In other words, malicious vehicles are added to the routing protocol because the trace file is generated from the malicious behaviour which has different characteristics from the trace file that had been generated from the normal behaviour. The self-driving vehicle is called malicious vehicle when it drops packets rather than forwarding them to the destination vehicle. Figure 4.16 shows a screenshot of ns-2 utilising NAM.

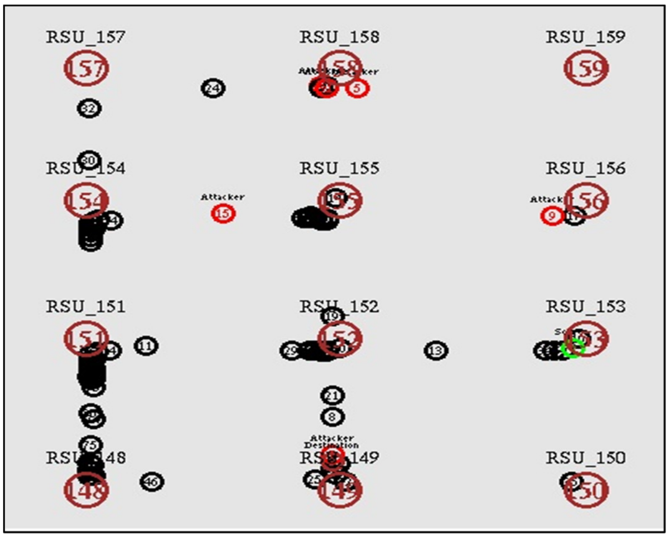


Figure 4.16 Screenshot of ns-2.

The external communication system of self-driving vehicles consists of 150 vehicles and 12 RSUs on a ns-2 simulator [88]. Six malicious vehicles are created to get different behaviour in VANETs.

d. Security Hash Algorithm 2

A hash function is an algorithm that maps data of arbitrary length to fixed length output (called the digest) [206]. Hash functions possess certain properties which makes them suitable for use in cryptography and security. For instance, it is not feasible to extract the input of a hash function if the output is provided. The second property of hash functions is that no two different inputs can have the same output. Owing to these properties hashing has been used in file authentication, user authentication, password storage, commitment protocols and digital signatures. Hashing algorithms are designed to be efficient which is why their use is preferred over symmetric key encryption. There are many popular hash algorithms like MD hashing, Simple Hash Function, RACE Integrity Primitives Evaluation Message Digest (RIPEMD) etc [207].

To utilise hashing for a system, a suitable one way hash algorithm is selected. The algorithm is supplied with an input x. The input is processed and produces the digest such that the digest cannot be used to recover the input x. Figure 4.17 below is a pictorial representation of this process. The hash algorithm here is SHA-2 that produces a digest of length 256bit.

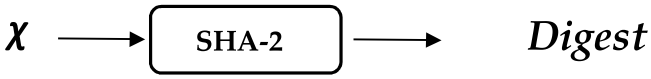


Figure 4.17 The SHA-2 Function.

e. Feature Sets and Extraction

The proposed authentication system and IDS rely on features that have been extracted from the trace file. It contains various data features that are employed for authentication and detection process. These features describe abnormal/malicious and normal behaviour in the external communication system of self-driving vehicles that are extracted from the trace file. The trace file consists of large and overlapping data that make extracting features from a trace file very complicated and difficult. To resolve this issue, the AWK and python language is utilised for the analysis and grip features which capture the behaviour of self-driving vehicles in real-world.

The data of the original trace file is divided into three parts: basic trace, IP trace, and V-AODV trace information [208]. However, we contributed to modify and add a new feature which is the hash ICMetric to the trace file: “message trace” information as shown in Table 4.5.

Table 4.5 Features of the Trace File.

Basic Trace	IP Trace	V-AODV Trace	Message Trace
Event	IP Source	Packet Tagged	$h(ICMetric)$

4.3.3 Simulation System

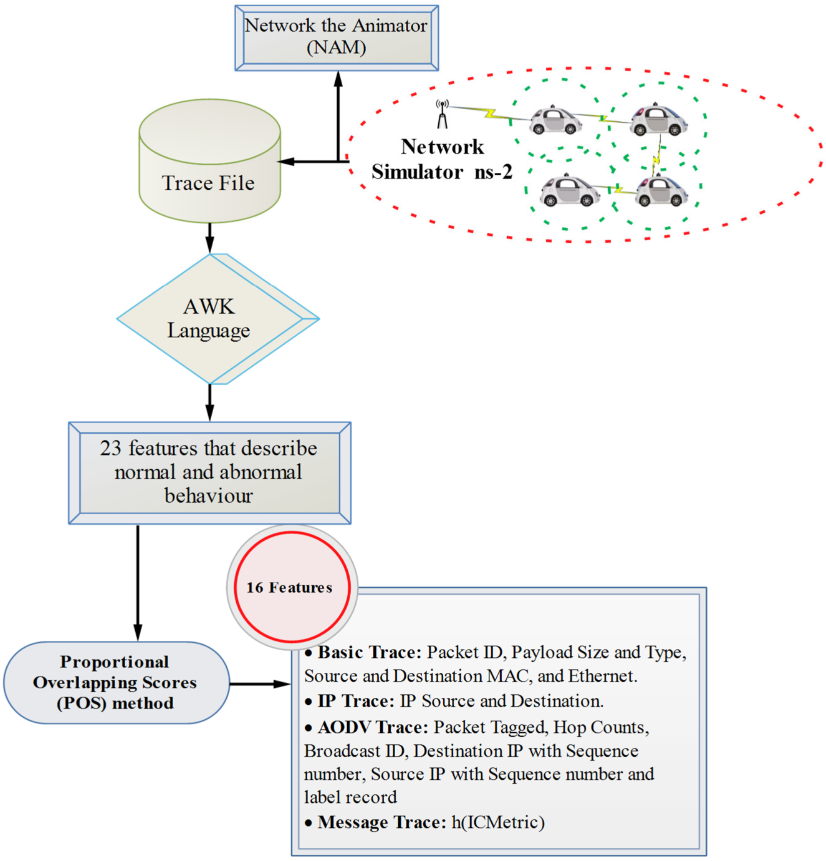
Time	IP Destination	Hop Counts
Trace level	Time to Live	Broadcast ID
Node ID	Next Hop	Destination IP with Sequence number
Packet ID		Source IP with Sequence number
Payload Size		
Payload Type		
Source MAC		
Destination MAC		
Delay		
Ethernet		
Flag		

The number of features that are produced from the trace file plays a vital role in the efficient performance and effectiveness of the proposed security system as well as ideal exploitation of memory, reduced computation time and increase in detection accuracy. We need to extract the most significant features based on the detection system to enhance and increase the efficiency and the accuracy of the IDS. In this chapter, a statistical method, POS, is utilised to extract a high-weight value of features from the trace file that was mentioned in detail in Chapter three [162].

The distinguishing extracted features are singled out by calculating the proportional overlapping score to avoid the outliers effect for each feature in the trace file. The selection process of relevant features is based on the measure for the overlap is the one defined in the POS method [209]. It is efficient and suitable with the data has common classification problem such as the outliers and high-dimensional binary [209]. The proposed IDS is based on the identification of features picked by measuring the overlapping rate between the features in the trace file across both classes: abnormal/malicious and normal. The statistical R language is employed in order to apply the POS method.

4.3.3 Simulation System

In our work, the principle of trial-and-error is used to choose the optimal number of features based on the accuracy rate. We started with the 23 features that describe the normal and malicious behaviour of self-driving and semi self-driving vehicles. We removed the feature which had the lowest weight after each round of training time. This process is repeated until the training rate is up to the highest accuracy rate. In other words, the best accuracy rate reaches at a set comprising of only 16 features. Figure 4.18 shows all the features, and significant features that are extracted from the trace file in VANETs.


Network the Animator (NAM)
Trace File
Network Simulator ns-2
AWK Language
23 features that describe normal and abnormal behaviour
16 Features
Proportional Overlapping Scores (POS) method

- **Basic Trace:** Packet ID, Payload Size and Type, Source and Destination MAC, and Ethernet.
- **IP Trace:** IP Source and Destination.
- **AODV Trace:** Packet Tagged, Hop Counts, Broadcast ID, Destination IP with Sequence number, Source IP with Sequence number and label record
- **Message Trace:** h(ICMetric)

Figure 4.18 The Flow Process to Extract and Select Significant Features.

These features are: Packet ID, Payload Size and Type, Source and Destination MAC, Ethernet, IP Source and Destination, Packet Tagged, Hop Counts, Broadcast ID, Destination IP with Sequence number, Source IP with Sequence number and *h*(ICMetric). They are used in the design of IDS to detect the malicious behavior of the normal in external communication of autonomous vehicles. To illustrate the efficiency of the 16 features, the performance is metrics compared with previous studies where the authors employed all extracted features from the trace file with our IDS [20]. Table 4.6 shows the performance metrics for the two sets of features. We can easily notice the vital role of the 16 features in enhancing the detection rate and reducing the training time as well as a decline in the error rate.

Table 4.6 Performance Metrics of ICMetric-IDS.

	IDS with all Features	IDS with 16 Features
Training Rate	98.97%	99.84%
Average False Alarm	6.21%	0.25%
Error Rate	2.05%	0.17%
Train Parameter Epochs	68	23

f. Fuzzification of the Benchmark

The features extracted from the trace file can have some data problems that describe the normal and abnormal behaviour. These problems have a direct impact on the detection rate and the number of false alarms of the proposed ICMetric-IDS. One of these problems is the ambiguity between the normal and abnormal/malicious behaviour if the name of the class is not well-defined or the distribution of the features is not clear. To overcome this problem, a mathematical model is utilised to develop solutions and redistribute the extracted features to build clear boundaries between them. The fuzzy set is used to fix the data problem because it is efficient, well-known and widely used in scientific fields [210].

This mathematical model is considered an optimal solution of the classification problem by employing a classification model on the significant features that were extracted from the trace file of ns-2 [98]. We could clearly notice the role of fuzzy set in improving the results of our proposed system, when comparing with our previous research where fuzzification was not used. In our experiments, we got the false alarm rate ranging from 0.17 to 12.24% [20]. We can easily observe the vital role of fuzzy set in enhancing the average detection and decreasing of false alarms. Each feature value is distributed in five values of fuzzy with a range in [0, 1] as shown in Chapter three.

Finally, utilising fuzzy data improves the detection rate of proposed IDS as well as reduces the number of false alarms that are generated from the intelligent IDS.

g. Intelligent Intrusion Detection System

An ICMetric-IDS is built that is based on FFNN and k-NN to identify/detect vehicles with a malicious behaviour in the external communication system of self-driving and semi self-driving vehicles. The most efficient tool in designing internal and external systems is ANNs [156]. The proposed security system utilises a data set of 60.000 records to reflect the normal and abnormal behaviour in VANETs. The collected data set was divided into three subsets collected from the trace file of ns-2: the test set, the validation set and the training set. The validation data set helps the intelligent detection system avoid over fitting.

The principle of trial-and-error and the best ratio of training neural network are considered the criteria for selecting the best configuration of the ANN used to design the proposed IDS. The best structure of the ANN that was nominated in our security system is shown in Figure 4.19.

4.3.3 Simulation System

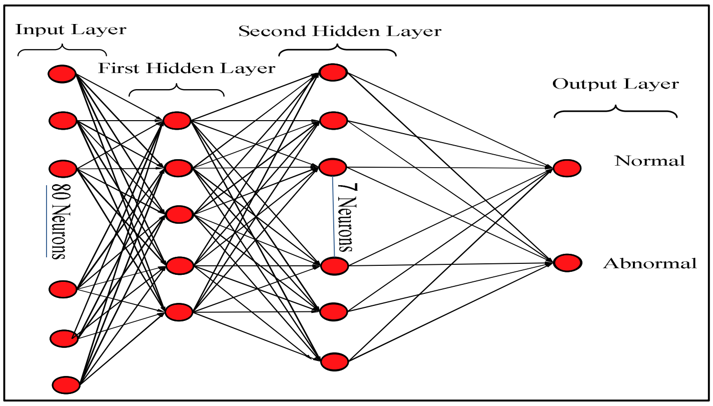


Figure 4.19 Structure of the ANN.

Table 4.7 shows the initial parameters of the training phase used in the ANN; these have a direct impact on the performance of detection.

Table 4.7 Initial Parameters of ANN.

Parameter	Value
Train Parameter epochs	23
Train Parameter learn	$1*10^{-7}$
Train Parameter goal	0
Train Parameter min_grad	$1*10^{-13}$
Gaussian Radial Basis Function	1
BoxConstraint	$1e^{6}$

The initial parameters of ANN play an important role on training accuracy and time consumption in the training phase of the proposed security system. In this system, epoch parameter is established with 500 epochs as stopping condition but according to Table 4.7, we can easily notice that ANN obtained the acceptance training rate with 23 epochs. As for the other the parameters identified in Table 4.7 and number of hidden layer are placed according to the trial and error principle with 99.84% average training rate.

The ANN consists of three layers: an input layer, a hidden layer and an output layer. The first layer input comprised 80 neurons equal to the fuzzified data set that was extracted from the trace file of ns-2 after employing a fuzzy set to them. The proposed security system is composed of two of the middle hidden layers that help to increase the detection rate and reduce the number of false alarms. They consist of five and seven neurons respectively, and the output layer comprises two neurons ("normal", "abnormal").

4.3.4 The proposed Intrusion Detection System

Providing sufficient security to protect the external communication system of self-driving and semi self-driving is the target of this thesis. Two security levels are designed which are the authentication phase and the anomaly detection phase.

A. Authentication Phase

A novel authentication system is proposed to secure the external communication system of self-driving vehicles. The authentication or identification phase is considered one of the most important security aspects that must be provided for each system. This phase assists the moving vehicles to distinguish between the authorised and unauthorised vehicles so that they can communicate with each other in that radio coverage area. In other words, this phase heavily depends on the ICMetric basis number that is generated from the bias readings of the sensors for self-driving and semi self-driving vehicles. Figure 4.20 describes the proposed authentication scenario for self-driving vehicles. The security system assumes that each vehicle has the hash value generated from the ICMetric basis number which is considered an identifying aspect for each vehicle in VANETs.

4.3.3 Simulation System

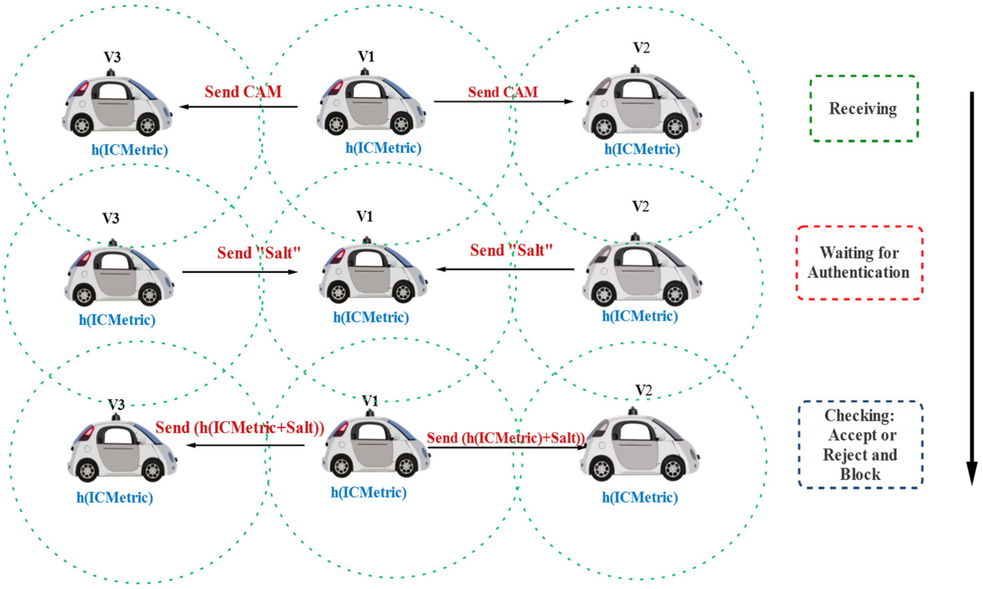


Figure 4.20 Authentication Scenario.

Definition- salt value: It is a random number that is integrated with CAMs from destination node to increase the security of communication between vehicles in external communication system.

The authentication scenario is as follows:

- The vehicle V_1 sends CAM to the vehicles V_2 and V_3.
- The Vehicles V_2 and V_3 send random value (salt) to the source vehicle (V_1) and wait.
- The vehicle V_1 sends summation of the salt value with *h* (ICMetric) value to the destination vehicles (V_2 and V_3).
- The vehicles V_2 and V_3 will match the received value with their own value. If the value matches the decision it “accepts the CAM”, otherwise they will “reject and block the communication with vehicle V_1”.

The algorithm 4.1 shows an algorithm for vehicles authentication that is proposed to secure the external communication for autonomous vehicles.

4.3.3 Simulation System

Algorithm – 4.1 : Vehicles Authentication

Input:

- Started when vehicles are within range of central transmission.
- Authorised vehicles are understanding the ICMetric number.
- Central Vehilce =v_1, client Vehicles =v_2, v_3, …. v_n.

Procedure:

1. Vehicle V_1 send CAM message to the fixed rang.
2. Authorised vehicles (with range) v_2 … vn send response message (salt) and wait.
3. Vehicle v_1 send summation (salt + h(ICMetric)) to the destination vehicles.
4. Destination vehicles will match the received value with own value.

Output:

- Accept communications if matching the received value.
- Reject communications if not matching the received value.

End

B. Anomaly Detection Phase

The proposed system first determines the ICMetric basis from the ultrasonic and MEMS sensors. The cryptographic hash function is applied on ICMetric basis to generate *h* (ICMetric). It is then integrated with CAMs from source node to the destination node. The behaviour features require a pre-processing phase and are then considered the input to the intelligent IDS. The IDS outputs are then considered normal or malicious connection.

The detection phase in the proposed security system has ten stages, and the overall architecture of the proposed IDS is shown in Figure 4.21.

4.3.3 Simulation System

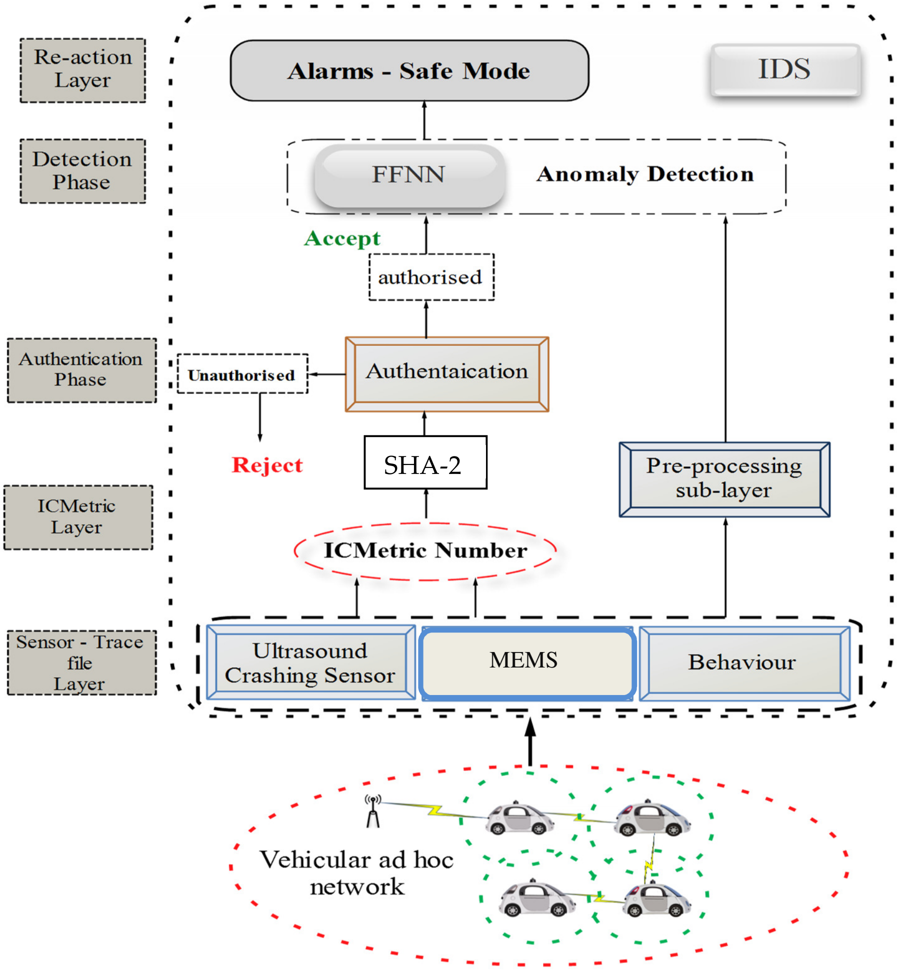


Figure 4.21 Overall Intrusion Detection of the Proposed Scheme.

- The first stage (extract bias reading and assume ICMetric basis number)- In this stage, the offset reading is extracted from the four sensors on self-driving vehicle. An assumed ICMetric is used to generate a hash from the ICMetric basis number which is employed in the proposed security system.
- The second stage (integrated hash ICMetric): The *h*(ICMetric) value is integrated with ns-2 trace file. In other words, the *h*(ICMetric) value is extracted with features from trace file. All these features are utilised in training and testing phases.
- The third stage (generate the real-world): The SUMO and MOVE are used to generate the mobility and traffic model in VANETs that reflect the real

movement of self-driving vehicles. The ns-2 uses the output files from these tools as input to generate a trace file that describes normal and abnormal.

- The fourth stages (ns-2): The output files generated from the third stage are used as input files for the ns-2. These files are the NAM file and the trace file; the normal and abnormal behaviours are simulated in this chapter.
- The fifth stage (significant feature extraction): In this stage, the features are extracted from the trace file which is generated in the fourth stage. The proposed IDS only utilises 16 significant features from all the features [166]. Decreasing the number of extracted features play a vital role in enhancing the detection rate and reducing the false alarms.
- The sixth stage (pre-processing dataset): The significant features were pre-processed to transfer some symbols to numbers, and to apply a uniform distribution to create a balance between normal and abnormal, and to increase the efficiency of the detection rate. The normalisation formula is applied on the output data to enhance the performance of ANN and k-NN by converting them to numeric values between 0 and 1 according to Equation 3.1.
- The seventh stage (fuzzification dataset): The output data set from the sixth stage has to be converted into fuzzified data. The fuzzification process can solve some common data problems that occur in the extracted dataset, such as overlap and lack of clarity between normal and abnormal.
- The eighth stage (training phase-FFNN and k-nearest neighbours (k-NN)): The FFNN-IDS and k-NN- IDS are trained with the fuzzified data that was generated in the seventh stage. The detection rate is obtained for normal and malicious/behaviour.
- The ninth stage (testing phase-FFNN and k-NN): The FFNN-IDS and k-NN-IDS are tested with the extracted dataset; the detection rate for normal and abnormal behaviour, and four types of alarm are calculated in this stage. There

are criteria for measuring the efficiency of ANN and k-NN. For example, detection rate, the number of false alarms, throughput, Packet Delivery Rate (PDR) and End-to-End delay, error rate and Standard Deviation.

- The tenth stage (re-action): The activeness of this stage depends on the results of these IDS. In other words, it is only active when the detection result is malicious vehicles. This stage tries to introduce the infected vehicles in the safe mode to save lives of drivers, passengers and vehicles themselves at suitable time without delay.

4.4 Experimental Results

Our experimental setup consists of a set of three ultrasonic and three myAHRS_plus sensors for creating ICMetric basis number that is utilised to secure the external communication system of self-driving vehicles from potential attacks. To get an accurate reading from the sensors, ultrasonic and MEMSs devices are placed in an environment free from magnetic and vibration interference.

The bias readings are obtained from the ultrasonic, accelerometer, magnetometer and gyroscope sensors to create the device ICMetric. A total of 6500 readings were recorded from the ultrasonic sensor and 1000 readings were recorded per axis from the MEMS sensors. The statistical analysis is done on the recorded data/offset reading to establish ICMetric basis number. As we mentioned, the cryptographic library is utilised to generate hash ICMetric value from the ICMetric basis number that is employed in authentication and detection phases for the proposed ICMetric-IDS. The hash ICMetric may have been included in the message content that was sent from the source to the destination. The proposed IDS is based on the trace file that contains all significant features such as, basic trace, IP trace, V-AODV trace and message trace.

In general, the proposed IDS may be installed in three configurations: RSUs, vehicles or both. In this chapter, the ICMetric-IDS is configured in self-driving vehicles that plays a vital role in identifying two different behaviours: normal and abnormal/malicious. In order to evaluate the performance of the proposed ICMetric-IDS, we need to calculate the performance metrics, detection accuracy and four types of alarms: TP, FP, TN and FN.

In this chapter, three ICMetric-IDS are proposed to secure the external communication system for autonomous vehicles which are: 1) ICMetric-IDS based on bias readings of ultrasonic and accelerometer sensors. 2) ICMetric-IDS based on bias readings of magnetometer sensors. 3) ICMetric-IDS based on bias readings of gyroscope sensors. In this case, we need to evaluate and test the proposed security systems under certain condition.

4.4.1 ICMetric-IDS based on Ultrasonic and Accelerometer Sensors

To test and evaluate the performance of the proposed ICMetric-IDS, we need to generate two types of scenarios normal /abnormal, and simulate these using ns-2 under certain conditions in order to obtain real data. In this case, we have ready significant features for the training and testing phase so as to measure the performance of the proposed security system. The average of the training algorithm is 99.61% in the training phase of our system.

In testing phase, the fuzzified data is used for testing the ability of the ICMetric-IDS in anomaly detection of different malicious behaviours in the external communication system of self-driving vehicles. In other words, the detection rate and the alarms are calculated for the proposed security system. The cross validation for FFNN and k-NN is employed to evaluate the performance of the proposed IDS. The data set is divided into 30 subsets (k=100) that had used 90% of the dataset in the training phase and 10% in testing phase. This process is repeated to measure the efficiency and effectiveness of the ICMetric-IDS by calculating the standard deviation

(SD), detection rate and time. Table 4.8 shows the number of records that were used in our system and detection accuracy rate.

Table 4.8 Accuracy of Classification.

Attack Class	IDS				
	Real Record	ANN	Match Records	Miss Records	Accuracy
Normal	9697	9649	9647	2	99.48%
Abnormal	5303	5324	5300	24	99.94%
Unknown	0	27	0	27	NaN

Table 4.9 shows the time, SD, error detection rate and four alarms that are generated in the testing phase of the IDS. These alarms are calculated by Equations 3.3, 3.4, 3.5 and 3.6.

Table 4.9 Alarm Rate.

Alarm Type	FFNN	Time/s	Error Rate	SD
True positive	99.9	3.48s	0.15%	0.074
True negative	99.8			
False negative	0.08			
False positive	0.19			

In addition, a criterion is required to measure the efficiency of the proposed system, and to clarify its role in improving the performance of VANETs. The proposed evaluation criteria are PDR, average end-to-end delay and average throughput [211]. The PDR, average throughput, average end-to-end delay and detection rate for packets in VANETs for three types of networks: VANETs without IDS under attacks, VANETs with Normal-IDS and VANETs with ICMetric-IDS are shown in Table 4.10.

Table 4.10 Performance Comparison of ICMetric-IDS.

Performance Metrics	Detection rate		Throughput	PDR	End-to-End Delay	False Alarm
	Normal	Abnormal				
VANETs without-IDS	--------	--------	1.02%	0.05%	23.33ms	--------
VANETs with Normal-IDS	98.45%	85.02%	78.57%	97.86%	1.47ms	12.24%
VANETs with ICMetric-IDS	99.48%	99.94%	80.34%	99.89%	101.63ms	0.19%

We can easily observe the role of the ICMetric-IDS on the external communication of self-driving vehicles/VANETs under different types of attacks. Finally, the four alarms are considered the first re-action technology for the self-driving vehicles.

4.4.2 ICMetric-IDS based on Magnetometer Sensors

In this experiment, the bias readings are generated from the three identical magnetometer sensors to establish the ICMetric basis number. These readings are employed in designing a novel ICMetric-IDS to identify internal/external attacks. In the testing phase, the extracted significant features are utilised to evaluate the anomaly detection in the external communication system for self-driving vehicles. The detection rate and false alarm of the proposed ICMetric-IDS with the traditional IDS as shown in Table 4.11.

Table 4.11 Detection Rate and False Alarm.

Performance Metrics	Detection Rate		False Alarm
	Normal	Abnormal	
VANETs with Normal-IDS	98.45%	85.02%	12.24%
VANETs with ICMetric-IDS	99.77%	98.78%	1.21%

In Table 4.11, the proposed security system achieves significant security improvement on the external communication system of self-driving vehicles under various types of attacks with average error rate of 0.72%.

The performance of the proposed ICMetric-IDS is shown in Table 4.12.

Table 4.12 Performance Metrics of ICMetric-IDS.

Performance Metrics	Throughput kpbs	PDR	Delay
VANETs without-IDS	1.02	0.05%	23.33ms
VANETs with Normal-IDS	78.57	97.86%	1.47ms
VANETs with ICMetric-IDS	80.22	99.64%	28.71ms

All the IDSs in Table 4.12 are tested under malicious conditions to calculate their performance. This IDS was formally presented in the form of a research paper at ICASE Conference, Newcastle, United Kingdom, 20-21 October 2016.

4.4.3 ICMetric-IDS based on Bias Readings of Gyroscope Sensors

Three gyroscope sensors were utilised to extract bias readings. The extracted readings demonstrated that a minimum of around 1000 samples are required to achieve a mean convergence point. In testing phase, the extracted data is employed for testing the ability of the IDS in identifying malicious behaviours in the VANETs. Table 4.13 shows the accuracy of detection, time, P-value and SD of the proposed ICMetric-IDS.

Table 4.13 Performance Metrics of ICMetric-IDS.

Class	Accuracy	Time	P-value	Standard Deviation
FFNN-ICMetric-IDS	99.83%	4.24s	8.6006E-09	0.02
k-NN-ICMetric-IDS	99.28%	68.4s		0.09

Table 4.14 shows the error rate and alarm rate.

Table 4.14 Alarm Rate of ICMetric-IDS.

FFNN-IDS	Accuracy	k-NN-IDS	Accuracy
True Positive	99.72%	**T**rue **P**ositive	99.76%
True Negative	99.89%	**T**rue **N**egative	99.01%
False Positive	0.09%	**F**alse **P**ositive	0.98%
False Negative	0.26%	**F**alse **N**egative	0.22%
Error Rate	0.16%	Error Rate	0.71%

According to the results in Table 4.14, ICMetric-IDS, that is based on FFNN algorithm, is more efficient, effective and has low error rate in detecting malicious vehicles as compared to ICMetric-IDS that is based on k-NN algorithm. This IDS was formally presented in the form of a research paper at the IEEE International Conference on Consumer Electronics (ICCE), Las Vegas - USA 2017.

4.5 System Analysis

The success and development of self-driving vehicles heavily rely on adequate security systems that provide a safe environment for external communication system /VANETs. The methodology used in designing the security system is summarised in ten phases: extracting bias reading, calculating the ICMetric basis number and generating and integrating *h* (ICMetric), establishing the real-world, the ns-2 to generate the trace file, data collection, pre-processing and extracting significant features, fuzzification of the extracted features, training phase-FFNN and k-NN, testing phase for the FFNN and k-NN and re-action technique - alarms.

In Table 4.10, 4.11 and 4.12, the performance and efficiency are compared of VANETs with and without the ICMetric-IDS. We can easily observe that the ICMetric-IDS was more efficient and effective in detecting malicious vehicles as compared to traditional IDS which is not based on the ICMetric technology. In addition, it has a low false negative alarm rate, high PDR and throughput rate. The significant features are selected based on our previous study [166]. Moreover, addition of a new ICMetric feature played an important role in enhancing the detection rate and reducing the number of false alarms in the performance of IDS. All these factors made the proposed IDS more efficient in securing the VANETs of self-driving and semi self-driving vehicles.

The average error rate for the IDS based on the ICMetric technology was 0.34%. The average alarm rate in our security system fluctuated between 99.80% and 99.57% with excellent and efficient accuracy. On the other hand, the average false positive alarm rate was low at about 0.61% which is a good indicator of the results. The number of sent, received and dropped packets in the external communication system for self-driving and semi self-driving vehicles are shown in Figure 4.22.

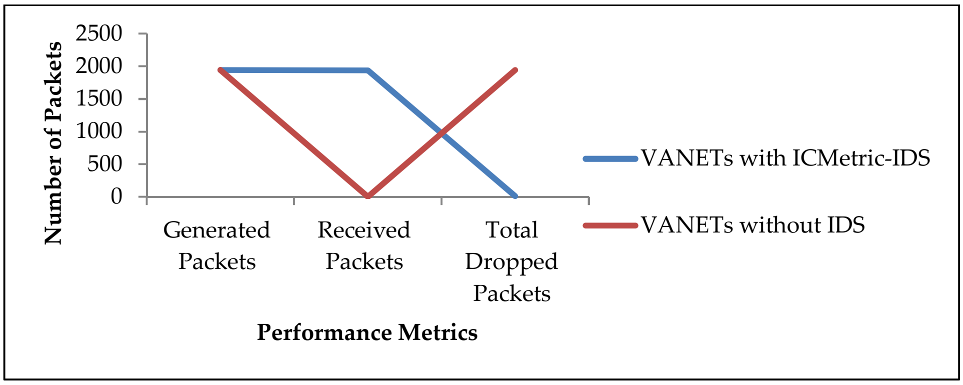


Figure 4.22 Number of Sent, Received and Dropped Packets in VANETs.

In Figure 4.22, the IDS is evaluated under attack condition: the total number of generated packets is 1944 packets in the two scenarios, while the number of received packets is 1937 in VANETs with ICMetric-IDS. Thus, the total number of dropped packets is 9 while 1 packet is received. Hence, the total number of dropped packets are 1943 in VANETs without IDS. In our experiments, we noticed that even smallest difference in bias reading extracted from the ultrasonic and accelerometer sensors is adequate for generating a stable ICMetric basis number.

Meanwhile, we can notice results in Table 4.13 that ICMetric-IDS that is based on FFNN algorithm is more efficient, effective, fast and has low error rate in detecting malicious vehicles as compared to ICMetric-IDS that is based on k-NN algorithm. The proposed ICMetric-IDS has demonstrated good performance in detecting and blocking malicious vehicle in VANETs of self-driving vehicles and semi self-driving vehicles.

4.6 Summary

An ICMetric-based vehicle sensing scheme is proposed in this chapter which employs ultrasonic crash sensors and MEMS accelerometer and other features to generate a novel vehicle identification called the vehicle ICMetric. One of the significant aspects of the ICMetric–IDS is its capability to detect both new and existing attacks. The ICMetric-IDS is considered a novel security system for securing external communication because this is the first time an ICMetric is used in VANETs. In our experiments, the proposed anomaly IDS has demonstrated good performance in identifying and blocking malicious vehicles in VANETs of self-driving vehicles. The process of decreasing the number of extracted features by POS method had a vital role in enhancing the detection accuracy and reducing the number of false alarms of the IDS, while the fuzzification process helps decrease the error rate and false alarms when compared with our previous research.

The experiments above have introduced a new effective security system, however, it may still needs to be improved with regard to the frequency of false alarms and the time span of the computational process. Above all, the system needs to be further improved in order to be quicker in response to security hazards. These improvements will be discussed and tested in chapter five below. New techniques will be employed in designing IDS to predict attacks on the communication system of autonomous vehicles which use FPN and clustering model.

CHAPTER FIVE

FUZZY PETRI NET INTRUSION DETECTION SYSTEM AND INTELLIGENT RESPONSE SYSTEM FOR AUTONOMOUS VEHICLES

"The only reason for time is so that everything doesn't happen at once"

Albert Einstein

Self-driving vehicles' movements and safety are dependent on the exchange of control and status data between vehicles and their roadside units. This information is exposed to several types of attacks, such as black hole, grey hole, Sybil and DoS. The challenge is to protect the communication systems of these vehicles from potential attacks. A novel security system is proposed in this chapter to protect the external communication of self-driving and semi self-driving vehicles. It can detect malicious vehicles in the urban mobility scenario. The anomaly detection system is based on a Fuzzy Petri Net (FPN) to detect most common attacks in vehicular ad hoc networks: packet dropping, Sybil and wormhole attacks. The Fuzzy Petri Net-Intrusion Detection System eliminates possible false alarms from the ordinary fuzzy model. The experimental results show that the proposed system can predict DoS attacks in external communication of self-driving vehicles. In addition, the anomaly detection is more efficient, accurate and real-time in identifying malicious vehicles.

According to the previous research, it was shown that FPNs can have a vital role in enhancing the security system used in different applications, such as wireless ad hoc networks [212]. FPN is the fusion of fuzzy logic and Petri nets. In other words, it is the combination of a mathematical model and a set of methodologies [213]. This combination makes it powerful and reliable in real-world scenarios. FPNs have a number of possible applications, such as control, scheduling, communication, decision-making and classification. In this research, FPN classification is utilised to distinguish between normal and abnormal communication.

In this chapter, three systems are proposed:

1) A novel security system based on FPN
2) A hierarchical IDS based on log
3) A new response system

The security systems are based on the FPN and clustering model to predict attacks on the external communications of autonomous and semi-autonomous vehicles. The FPN security system has the ability to identify and block a malicious vehicle among other vehicles. The detection system relies on a number of features that have been calculated from a trace file. It was generated using the network simulator software [98]. These features are the fuzzy parameters for the proposed security system.

5.1 Fuzzy Petri Net

Petri nets are utilised in many research applications. However, the rapid industrial development prevents the adoption of the petri nets because of their limitations in performing certain tasks like their inability to detect zero tokens and to support the design of large models [214]. This encouraged researchers to combine Petri Nets with Fuzzy Logic to create a new tool, the FPN [214]. FPN techniques are popular because they can produce precise outputs by removing ambiguities in data [215]. In addition, many researchers prefer FPN in decision-making processes, especially when ordinary algorithms are unable to describe the situation and multiple criteria utilised [216]. Also, FPN is straight forward to understand because the fuzzy logic uses natural language [217] as well as having tolerance and flexibility for data. In

FPN, many different membership functions are employed, such as Triangular, Trapezoidal, or Gaussian membership functions [218].

The FPN has two types of nodes: place and transition nodes. In FPN, a transition provides connectivity between a place node which holds a place token range (0-1). The FPN has the following attributes that make them suitable for this problem [219]:

- It allows researchers to visualise the structure of the proposed model making them clearer and easier to understand.
- It permits designers to use mathematical forms to describe the behaviour of the proposed system.

Fuzzy logic used formalism on Petri Nets to implement reasoning algorithms [214]. In Petri Nets, propositions and rules are represented in places and transitions respectively, whereas a truth table is represented in tokens. In addition, the firing process is defined as moving from one place to another by a transition connection.

Algorithm 5.1 – Constructing Linguistic Variables of FPN Model

```
begin
//Create group of rules to describe the knowledge of the security problem
For R (rule) Do
  Create a set of T (transitions)
        //Test each antecedent- consequent proposition
         While each of antecedent-consequent proposition Do
           Generate a set of P (places)
            $\alpha$(pi)= $yi$;
// where $yi$ is the degree of truth of proposition di.
            // Input values (arcs from Antecedents to T)
              Create a set of I: P× T→ [0,1].
               // Output values (arcs from T to consequents)
               Create a set of O: P× T→ [0,1].
            End While.
    End for.
    End.
```

The algorithm shows a set of linguistic variables that have been inferred from the fuzzy model. These variables describe the inputs to the FPN and the outputs obtained processing [220].

The FPN pass life cycle is divided into four phases [213]:

- Fuzzy set definition
- Fuzzy rule base
- Fuzzy inference engine
- Defuzzification

Figure 5.1 depicts the block diagram of FPN to predict DoS.

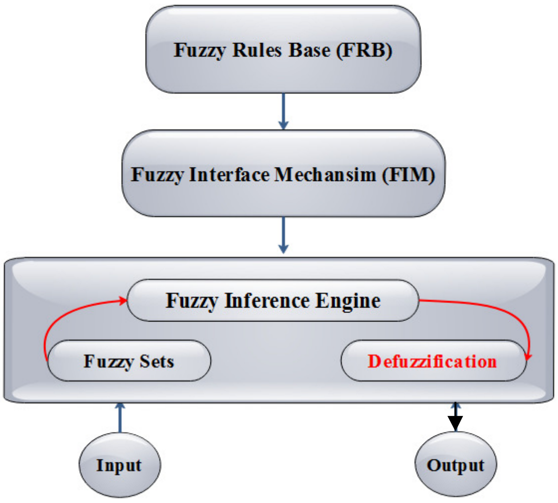


Figure 5.1 Block Diagram of FPN.

5.2 Intrusion Detection System Based on Fuzzy Petri Net

Ad hoc networks have particular characteristics that make conventional security systems inefficient in VANETs [221]. Therefore, there is significant attention from researchers to develop current security to become more suitable to protect inter and intra-vehicles communications. In this chapter, an intelligent security system is built which employs FPN to detect malicious vehicles based on parameters that reflect the vehicles' behaviour on roads.

5.2.1 Mobility Model for Self-Driving Vehicles

In VANETs, the mobility model is considered important in creating a simulation environment for self-driving vehicles. The challenge lies in how to build an environment close to the real world. In order to establish a real environment for vehicles, two platforms are used: SUMO and MOVE [19]. This structure allowed the network simulator to generate different scenarios, such as a Simple Model (SM), Manhattan Model (MM) and Downtown Model (DM). The mobility model used in this chapter is MM. It has some properties that encourage researchers to select it in their project, such as flexibility in selection of direction of vehicles as well as its wide adoption in investigation and research [19].

5.2.2 Normal and Abnormal Behaviour

The performance of the proposed security IDS needs to be evaluated in two of scenarios: normal and malicious behaviour. To create malicious behaviour, two source files are modified to exemplify a packet dropping attack. The specific malicious vehicles will drop packets rather than forwarding them to the destination vehicles. This type of attack has a direct and negative impact on the performance of VANETs. Each node corresponds to one vehicle in this scenario. In this proposal, two nodes are made malicious vehicles. The MM consists of 38 normal vehicles, two malicious vehicles and nine RSUs.

5.2.3 Fuzzy Parameters

Fuzzy parameters are used as input values for the proposed security system. In this case, some parameters are extracted from VANETs that describe the normal and abnormal behaviour for self-driving vehicles in network simulator. These parameters are:

- The average of the Delivery Packet Rate (PDR): it indicates the efficiency of performance for VANETs.
- The average of Dropping Packet Rate (DPR) on VANETs: the proposed system needs to calculate the proportion of dropped packets with period transfer from source to destination. In this case, the attacker tries to drop sent packets rather than forwarding them to destination vehicles, so DPR is used as an input parameter for the proposed security normalisation.

The number and type of detection features are heavily based on attacks types. In addition, the security system is proposed in this chapter to detect flooding and dropping attacks. In this case, the system requires features that measure flooding and dropping rate which are PDR and DPR. These features play direct and important role with the proposed security system.

Many studies recommended normalising values that are used in artificial intelligence techniques [222]. In this phase, the input values are converted to fuzzy between 0 and 1. Figure 5.2 the fuzzy input membership functions as a function of a normalised attack level.

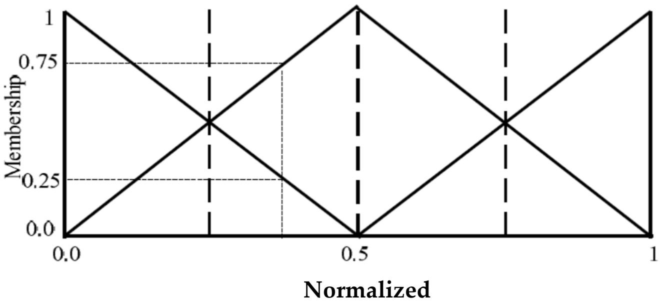


Figure 5.2 Normalized Attack Level.

5.2.4 Rules Sets

The proposed IDS uses nine rules to achieve its role. These rules are considered the core of FPN for accurate and efficient detection of the attacks. Table 5.1 shows these rules for Verity Level (VL):

Table 5.1 Parameters Definition of the Nine Qualitative Fuzzy Rules.

Rule's Serial No.	Rule Description
R_1	If PDR is "Low" and DPR is "Low" then VL shift is "Low"
R_2	If PDR is "Low" and DPR is "Medium" then VL shift is "Low"
R_3	If PDR is "Low" and DPR is "High" then VL shift is "Low"
R_4	If PDR is "Medium" and DPR is "Low" then VL shift is "Medium"
R_5	If PDR is "Medium" and DPR is "Medium" then VL shift is "Medium"
R_6	If PDR is "Medium" and DPR is "High" then VL shift is "Low"
R_7	If PDR is "High" and DPR is "Low" then VL shift is "High"
R_8	If PDR is "High" and DPR is "Medium" then VL shift is "High"
R_9	If PDR is "High" and DPR is "High" then VL shift is "Low"

5.2.5 Fuzzification

Fuzzification is the first step in the FPN algorithm. In this chapter, the proposed system utilises a triangular membership function, defined formally as Equation 5.1. The fuzzy variable deviation consists of three fuzzy sets, i.e. low, medium and high. In other words, fuzzy set is employed to calculate low, medium and high value.

$$f(x,a,b,c) = \max(\min(\frac{x-a}{b-a},\frac{c-x}{c-b)}),0) \tag{5.1}$$

where x is the actual value of parameters, whereas a, b and c are parameters which represent fuzzy domain values. Equation 5.1 will be applied to all values to generate three values for each value. Thus, the value of the fuzzy are calculated and set based on the Mamdanis fuzzy inference method [21]. Figure 5.3 shows the triangular membership function.

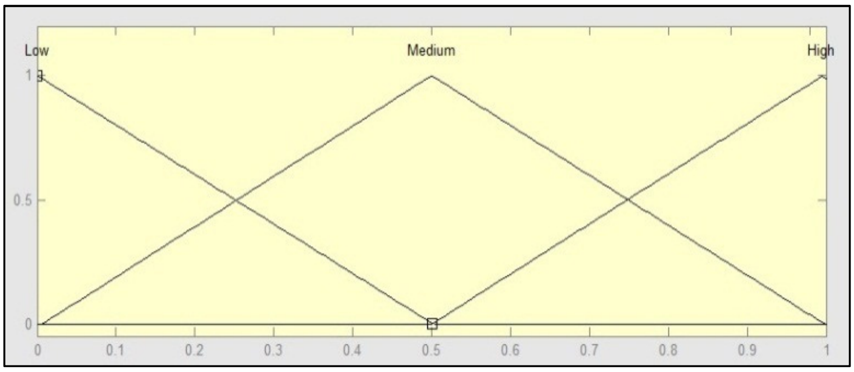


Figure 5.3 Data Fuzzification.

Equation 5.1 is applied to all values to generate three values for each value. In other words, we calculate the value of fuzzy set based on the Mamdanis fuzzy inference method. The behaviour of attacks and networks plays a critical role in determining the value of the threshold. The value of the threshold determines the percentage accuracy of alarms rate that is generated from ns-2.

5.2.6 Defuzzification

Defuzzification translates the linguistic value of the output variable back into a real value representing the current value of the parameters. The membership function represents the relationship between the linguistic values and the corresponding real values:

$$R_{max,medium,min} = (r_1, r_2, r_3, r_4, r_5, \dots \dots . . r_9,)$$

$$Predict\ Value\ of\ DoS = \frac{\sum_{i=0}^{n} u[i] * y_i}{\sum_{i=0}^{n} u[i]} \tag{5.2}$$

where: u^i is the height value of output values and the y^i is the gravity's horizontal coordinate of output generated from the *i-th* rules; whereas n is the total number of matching rules for given values of each input dimension [220].

5.2.7 Simulation Environment

In this research, a network simulator is utilised to evaluate the performance of the proposed IDS. It is a popular simulator that is widely used for network research. The simulation results are a NAM and trace file. The trace file describes all network events between vehicles and RSUs in that zone. The IDS heavily depends on features that have been calculated from the trace file. These features are considered fuzzy parameters for FPN. The following features are used in this proposal: PDR and DPR. The behaviour and the performance of the proposed security system are determined by the initial parameters that are used in network simulator.

The efficiency of the proposed FPN-IDS is evaluated using a network simulator under two conditions: VANETs with FPN-IDS and VANETs without FPN-IDS. In this case, the performance metrics are calculated of VANETs in both conditions for self-driving and semi-self-driving vehicles, for instance, PDR, average end-to-end delay and average throughput [160].

- Packet Delivery Rate (PDR): the rate between the number of packets generated or sent from the source vehicle and the number of packets received at the destination vehicle.
- Throughput: the total number of packets that are transferred in the VANETs. This metric is used to calculate the effectiveness of the routing protocol in VANETs.
- Average End-to-End Delay: this metric is used to calculate the average packet delay based on time. In other words, the average time for the packets to reach the destination from the source.

5.2.8 Intelligent Security System

The sending and receiving of the CAMs over a shared communication channel between vehicles and their RSUs is an effective method for identifying the malicious behaviour in VANETs.

Figure 5.4 shows the architecture of the proposed IDS:

- The first stage: extracting fuzzy parameters (PDR and DPR). These parameters are extracted from the trace file which is generated from network simulator.
- The second stage (normalisation and fuzzification): the IDS needs to normalise the values of PDR and DPR. Fuzzified values are created from the normalisation step to complete the proposed system.
- The third stage (rules): at this stage, the fuzzy rule is applied. The proposed system has two inputs (fuzzy parameters), but it has one output (Certainty level).
- The fourth stage (FPN): the system applied the FPN based on Equation 5.3 [220]:

$$R_i = \min(a_{j1}, a_{j2}, a_{j3}, a_{j4}, a_{j5}, a_{j6}, \dots \dots \dots \dots \dots .., a_{jn}) * [i] \tag{5.3}$$

where R_i are rules, αjn represents the value of each place in the model, whereas the $[i]$ or confidence degree factor $CF = 1$ for all the transitions.

- The fifth stage (Defuzzification): it translates the output variable back into a real value:

$$\Pr edict\ value\ of\ \ DoS = \frac{0.0285 * 0.333 + 0.696 * 0.666}{0.0285 + 0.696} = 0.6625$$

- The sixth stage: IDS can detect the malicious behaviour at this step; it is based on the FPN.

The proposed security system is illustrated in Figure 5.4.

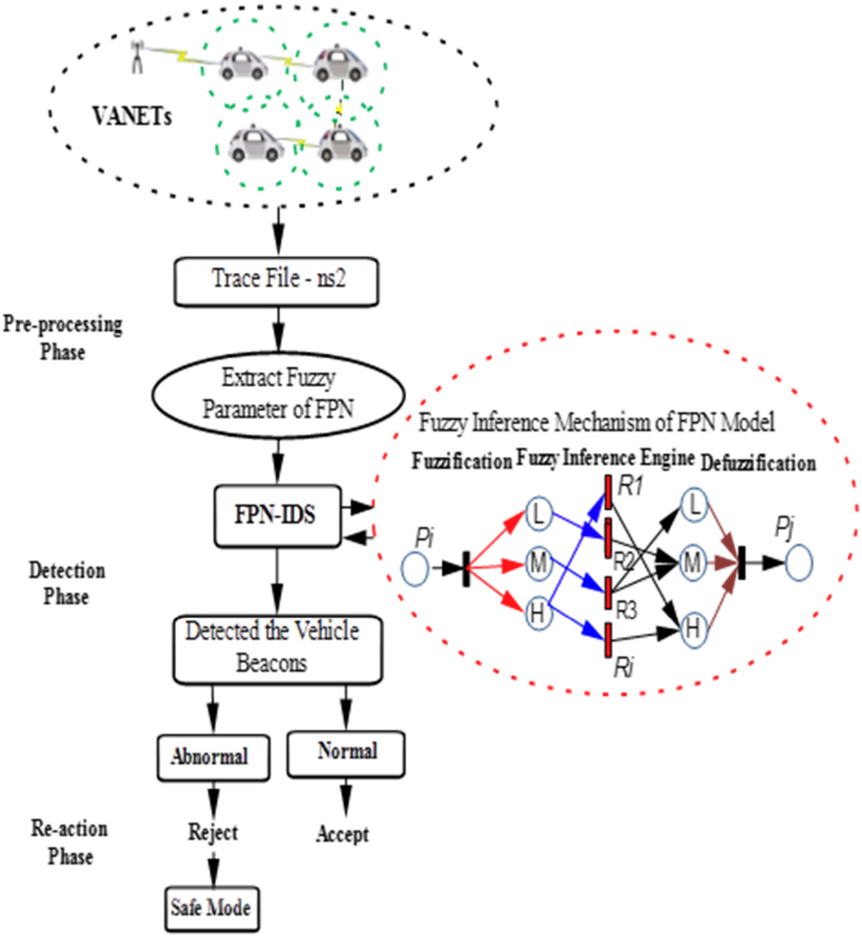


Figure 5.4 System Architecture.

The FPN-IDS system starts with producing the fuzzy parameters. They are fuzzified, and then processed based on an inferencing engine utilising nine rules. The output value is defuzzified and is compared with a threshold value to predict normal or abnormal behaviour.

5.2.9 Experimental Analysis

In order to evaluate the performance of the proposed FPN-IDS, the proposed security system is examined with different scenarios that describe the normal and abnormal behaviour of external communication of self-driving vehicles.

The steps explain the methodology for examining the detection system:

- Generate mobility and traffic model with two tools (SUMO and MOVE).
- Create malicious behaviour for some vehicles by modifying some files on the routing protocol.
- Calculate PDR and DPR used as input of fuzzy parameters.

According to Equation 5.1, the system can generate fuzzification of fuzzy parameters:

$PDR_{normal}= 0.825$; $DPR_{normal}= 0.175$

$PDR_{low}= 0$; $PDR_{medium}= 0.35$; $PDR_{high}= 0.65$

$DPR_{low}= 0.35$; $DPR_{medium}=0.65$; $DPR_{high}= 0$

1. Applying FPN based on Equation 5.3.

R_1= Min (0, 0.35) = 0

R_2= Min (0, 0.65) = 0

R_3= Min (0, 0) = 0

R_4= Min (0.35, 0.35) = 0.35

R_5= Min (0.35, 0.65) = 0.35

R_6= Min (0.35, 0) = 0

R_7= Min (0.65, 0.35) = 0.35

R_8= Min (0.65, 0.65) = 0.65

R_9= Min (0.65, 0) = 0

2. Defuzzification:

P_{7_Low}=Max (R_1, R_2, R_3, R_6, R_9)

Max (0, 0, 0, 0, 0) = 0

P_{8_Meduim}=Max (R_4, R_5)

Max (0.35, 0.35) = 0.35

P_{9_High}=Max (R_7, R_8)

Max (0.35, 0.65) = 0.65

The value of certainty level= (0*0.25+0.35*0.5+0.65*0.75)/ (0+0.5+0.65)= 0.6625

Hence, the final change is decided in certainty level will be "Medium". To verify the efficiency of the proposed security system, the FPN-IDS is tested in different scenarios. The normal and abnormal behaviours are represented as an input in Table 5.2 as well as the output, where normal is denoted by (N) and abnormal is denoted by (A):

Table 5.2 Testing FPN-IDS

Input		**Output**	**Class**
PDR	DPR		
1	0	*0.5*	N
0.8024	0.1975	0.75	N
0.3580	0.6419	0.362	A
0.8148	0.1851	0.75	N
0.6172	0.3827	0.636	N
0.3703	0.6296	0.386	A
0.7777	0.2222	0.75	N
0	1	0.25	A
0.0617	0.9382	0.25	A
0.5308	0.4691	0.572	N
0.2716	0.7283	0.312	A
0.7407	0.2592	0.75	N
0.9259	0.0740	0.75	N
0.0370	0.962	0.25	A

	9		
0.5308	0.4691	0.572	N
0.5925	0.4074	0.62	N
0.3086	0.6913	0.344	A
0.9012	0.0987	0.75	N
0.4444	0.5555	0.75	N
0.1358	0.8641	0.25	A

The classification rate is calculated of the proposed system as shown in table 5.3 and 5.4:

Table 5.3 Classification Rate of FPN-IDS.

Class	Accuracy	P-value
Normal	58.33%	
Abnormal	100%	0.000107
Threshold	0.66	

Table 5.4 Testing FPN-IDS.

Normal Behaviour		Abnormal Behaviour	
PDR	82.5%	PDR	30%
DPR	17.5%	DPR	70

The proposed system is simulated by gradually increasing the number of iterations. As the number of iterations increases, the stability of the accuracy increases. Figure 5.5 shows that the accuracy stabilises when the number of iterations exceeds nine.

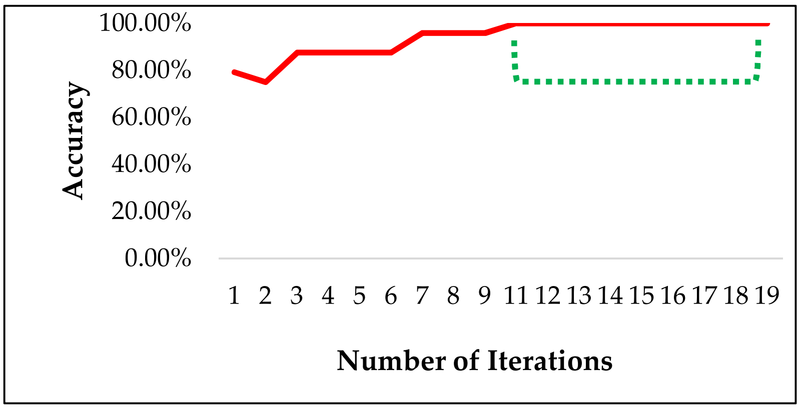


Figure 5.5 Graph showing the Relationship between the Number of Iterations and the Resulting Accuracy.

The proposed detection system become more accurate and stability when number of iterations exceeds nine is shown in Figure 5.5. The rate of four types of alarms is shown in Table 5.5.

Table 5.5 Alarms Rate of FPN-IDS.

Alarm	Accuracy
True Positive (TP)	72.22%
True Negative (TN)	100%
False Positive (FP)	0%
False Negative (FN)	27.78%

The performance metrics are evaluated of VANETs with or without the FPN-IDS for self-driving and semi-self-driving vehicles. The metrics are PDR, Average End-to-End Delay and Average Throughput. Table 5.6 shows the performance metrics of FPN-IDS:

Table 5.6 Performance Metrics.

Performance Metrics	VANETs with FPN-IDS	VANETs without FPN-IDS
PDR	98.31%	32%
Throughput	79.98%	31.07%
End-to-End Delay	213.17s	8.28s

The threshold value plays an important role in enhancing the detection rate and reducing the amount of false alarms [119], [223]. To select the optimal value of threshold, the FPN-IDS is tested with different values of threshold to calculate the accuracy of detection rate and false positive alarm. In this system, the threshold value is set to 0.42 because the most suitable threshold of certainty level lies between 0.38 and 0.48. The rate of detection with different thresholds is shown in Figure 5.6.

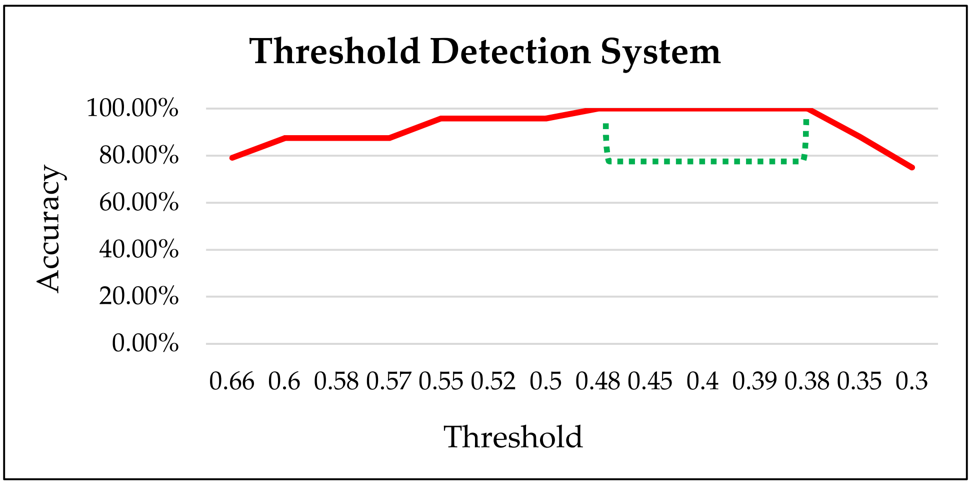


Figure 5.6 Dependency between Detection Rate and Threshold Value.

5.3 Response Mechanism

Security and privacy are considered very important matters of transport systems as they directly impact the lives of drivers and passengers. Security systems alone are not enough to provide sufficient security and safety, and alternative ways must be found to create a safe environment for any emergency situation. In this chapter, a time efficient system is developed so that a ‘safe mode’ can be induced in a compromised vehicle without delay. In other words, a quick response can be provided on the data link layer for any abnormal situation to prevent potential risks or hazards.

A new response system is considered as a communication protocol of self-driving vehicles under different conditions in order to facilitate a safe mode or a secure communication environment. A typical external communication of self-driving vehicles consists of three main entities in Manhattan scenarios that were established in a city street environment. In other words, it allows mobile nodes to move in urban conditions [151].

Trust Authority (TA), mobile On-Board Units (OBUs) equipped on each vehicle and immobile RSUs at the roadside every 250m as illustrated in Figure 5.7 [224].

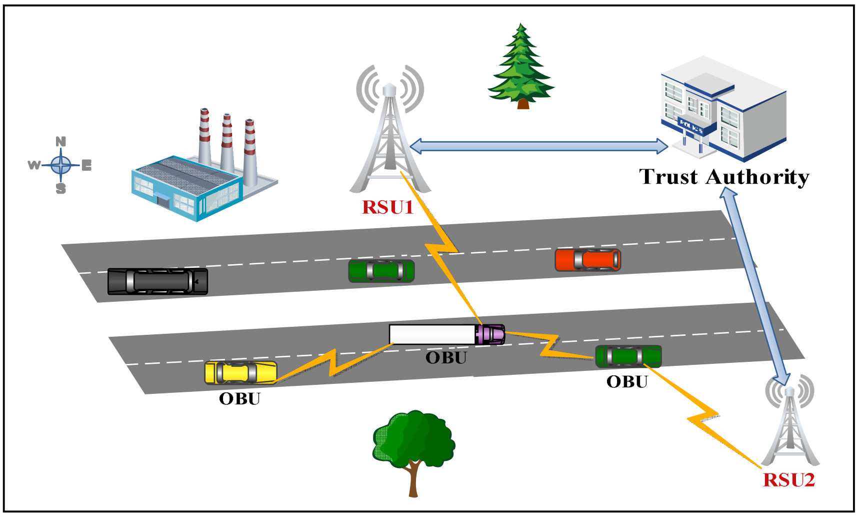


Figure 5.7 System Model.

The motivation of the proposed response system is to preserve the lives of drivers, passengers and vehicles themselves. The author is trying to increase the confidence of consumers in the acquisition of this new generation of vehicles. In addition, the reasons below encourage selecting certain RSUs in an emergency [224]:

- Trust because of its wire connection to TAs.
- Low delay.
- Low bit error rates.
- High bandwidth.

The IEEE 802.11p protocol has a problem in its scalability rate. In dense road scenarios, it is unable to provide the required time-probabilistic characteristics. In other words, it has low scalability when the self-driving vehicles are in the same area [225], [226]. All these features encourage us to make the RSUs the end-point of self-driving vehicles safe from any critical or emergency case.

5.3.1 Data Link Layer

The data link layer has many factors that encourage the designers to build the response mechanism within [227]:

- It supplies basic addressing and access control to the physical layer on VANETs of self-driving and semi-self-driving vehicles.
- It provides easy mobility of vehicle communication among the subnet, without requiring re-configuration.

These factors are considered the main reasons for selecting this layer among others on VANETs. In this layer, many types of communication protocols are used, such as the Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC) and Advanced Data Communication Control Protocol (ADCCP) [228]. The proposed response system is based on the PPP concept: "vehicle to the closest RSU".

5.3.2 Safe Mode

The safe mode is a protective response system that intervenes when a vehicle has been compromised. After a vehicle is compromised its ability to communicate with other vehicles in the same coverage area is restricted. The restriction allows the vehicle to only communicate directly with the RSU. The safe mode enforces a partial isolation policy, so that the functionality of the vehicle can be fully restored through interaction with the RSU. The vehicle cannot further disrupt the communications of other vehicles.

5.3.3 Testing Response System

In this subsection, normal and abnormal behaviours of self-driving and semi-self-driving vehicles are analysed. All behaviours of vehicles, whether benign or malicious, are based on a network simulator. An emergency connection protocol of these vehicles is proposed as a secondary communication system for any compromised situation. The safe mode places vehicles in an isolated state so that correct functionality can be restored. The proposed response system was evaluated under normal conditions. One of the self-driving vehicles is programmed with the new response system. The performance metrics are calculated for a vehicle in two cases under the same condition.

Table 5.7 shows the performance metrics that have been calculated for the same vehicle under normal behaviour with and without the proposed response system.

Table 5.7 Performance Metrics of Normal Behaviour.

Performance Metrics	Without Response System	With Response System
Generated Packets	14402	14402
Received Packets	12831	13654
Packet Delivery Rate	89.09%	94.80%
Totally Dropped Packets	2652	906
Average End-to-End Delay	120.10*ms*	62.61*ms*

On the other hand, Table 5.8 shows the performance metrics that have been calculated for the same vehicle under abnormal behaviour with and without the proposed response system.

Table 5.8 Performance Metrics of Abnormal Behaviour

Performance Metrics	Without Response System	With Response System
Generated Packets	14402	14402
Received Packets	7297	12622
Packet Delivery Rate	50.66%	87.64%
Totally Dropped Packets	7311	2602
Average End-to-End Delay	38.43*ms*	15.003*ms*

The performance of the proposed response system is measured under malicious behaviour. According to Table 5.8, the active role of the proposed response system can be easily distinguished in two cases of self-driving vehicles.

5.4 A Hierarchical Detection Method Based on TDMA

In this section, a hierarchical intrusion detection method is proposed to secure the external communication system of self-driving and semi-self-driving vehicles from the potential attacks. It is based on Cluster -Time Division Multiple Access (TDMA) to overcome some of problems of VANETs. These problems are: large density of vehicles on roads, high dynamic mobility and low bandwidth for exchanging beacons messages between them.

In this proposed IDS, each vehicle logs, calculates and stores various parameters that are calculated from trace file and log data after a significant period. If a vehicle has the same values for the log parameters at the same time with other vehicle, these vehicles are detected as Sybil attacks while the proposed system uses other parameters to detect wormhole attacks. The proposed system is based on parameters which describe the behaviour of vehicles, whether normal or abnormal. In other words, the IDS attempts to build a clustering approach that increases the system accuracy and efficiency, while providing a low false alarm rates in online detection. TDMA is used to provide channel access which shares medium networks based on splat signal between nodes in that radio coverage area. It divides the signal between vehicles' network into various time slots. In this chapter, an IDS is proposed to detect Sybil and wormhole vehicles. Figure 5.8 shows behaviour of Sybil and wormhole attacks in VANETs.

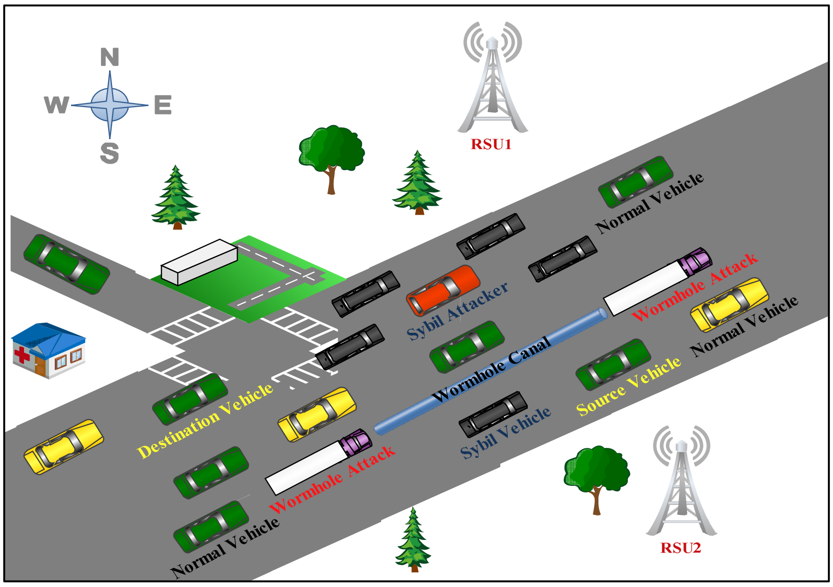


Figure 5.8 Typical Sybil and Wormhole Attacks in VANETs.

The proposed security system utilises the TDMA Cluster-based media access control to secure the VANETs for driverless vehicles. To achieve stability and channel utilisation, a cluster is needed in the external communication systems. The TDMA has the ability to divide signal into time frames and then into time slots, where each vehicle is associated with a time slot in the frame [229]. The IDS can detect and analyse the positions and IDs to calculate distance and angle of vehicles based on Cluster - TDMA. This can be relied upon to determine a malicious vehicle in the VANETs.

5.4.1 Clustering Mechanism

The proposed IDS is built on centralised authority to overcome a wireless network problem which is the lack of fixed security. In other words, the proposed security system is created on virtual centralised or semi-centralised authority by incorporating clustering [229]. Clustering based TDMA architecture provides the external communication system of driverless vehicles while offering scalability and fault tolerance resulting in efficient use of VANET resources.

The Clustering-Head (CH) receives data traffic and control data from Cluster Members (CMs) to validate malicious behaviour and generate alarms. The selection of the CH is based on selection algorithms which are used in clusters [229]. The semi centralisation optimises communication between vehicles and between vehicles and their RSUs. Figure 5.9 shows the taxonomy of existing clustering scheme for VANETs [229]:

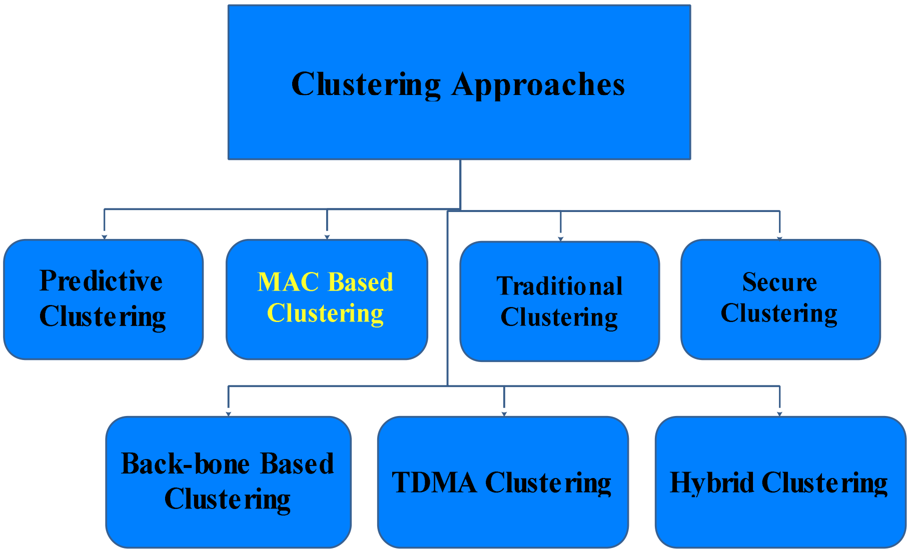


Figure 5.9 Taxonomy of Clustering Scheme.

A MAC algorithm is utilised in the TDMA method to reduce the number of packet drop, collision and enable vehicles to transmit on the same frequency channel by using clustering vehicles. Figure 5.10 shows the clustering scheme in the external communication systems.

5.4.2 Time Division Multiple Access (TDMA)

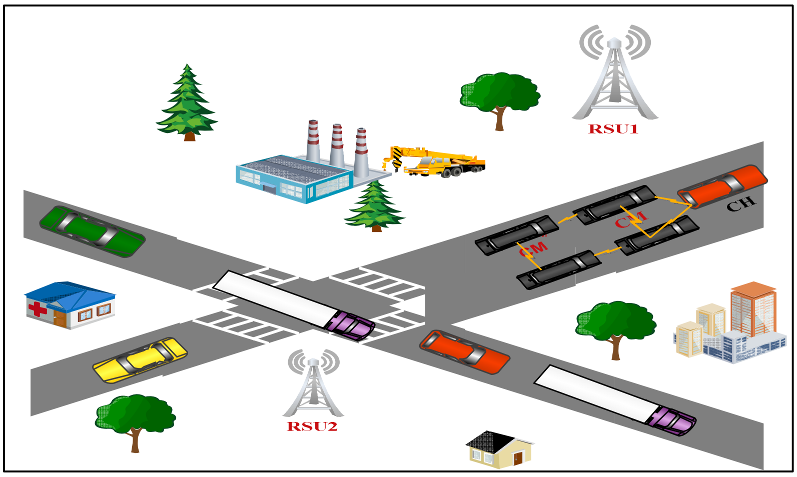


Figure 5.10 An Example of the Clustering in VANETs.

5.4.2 Time Division Multiple Access (TDMA)

TDMA is utilised to control channel access between vehicles by sharing a medium communication based on divide signal between nodes in that radio coverage area. It divides the signal between users by allocating different time slots. In this chapter, intrusion is based on clustering head (CH) vehicles. The security system uses the TDMA Cluster-based media access control to secure the VANETs for self-driving vehicles. To achieve stability and channel utilisation, the cluster is required in the external communication system. The TDMA divides signal into time frames, and it divides the time frame into time slots, where each vehicle is associated with a time slot in the frame [229]. Figure 5.11 shows the working of TDMA.

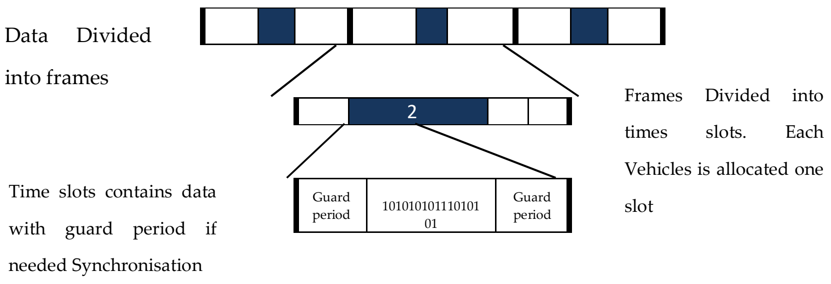

Data Divided into frames
2
Frames Divided into times slots. Each Vehicles is allocated one slot
Guard period
101010101110101 01
Guard period
Time slots contains data with guard period if needed Synchronisation

Figure 5.11 TDMA Structure.

5.4.2 Time Division Multiple Access (TDMA)

In addition, the TDMA can offer fairness in the sharing of communication channels between vehicles without employing any extra infrastructure or virtual leader vehicle [229]. To create a robust security system, two important challenges are addressed in this chapter: fuzzy logic and clustering based TDMA.

5.4.3 Intrusion Detection System Parameters

The accuracy detection and false alarm rate depend on the number and type of parameters that are utilised while designing the detection scheme [230]. In this system, four types of parameters are used: routing table, distance, timestamp and forward value (F_v). To get these parameters, each vehicle must collect data from its neighbour vehicles in inter-clustering. The following parameters describe normal and abnormal behaviours of self-driving vehicles in VANETs:

A. Routing Table

The routing table provides communication data of any vehicle whether in intra-clustering or inter-clustering of autonomous vehicles. In this proposed system, each vehicle has an IDS to sniff, analyse and identify normal/abnormal behaviours. It is required to write a function in the rtable.c file or routing protocol to generate a routing table. Table 5.9 shows basic information of routing table generated in ns-2.

Table 5.9 Routing Table.

Notation	Value
Vehicle ID	2
Current Time	1.00949s
Destination ID	3
Next Hop	3
Number of Hops	1
Sequence Number	4
Expire Time	7.0009s
Flags	1

5.4.2 Time Division Multiple Access (TDMA)

IDS installed on each vehicle will extract vehicle ID, time and number of hops from routing table to detect wormhole attacks.

B. Distance and Angle of Vehicles

A measure of distance between vehicles is an important factor in this proposed IDS. Each self-driving vehicle in clustering mode can calculate distance between itself and other vehicles, based on the values of x-axis and y-axis obtained from GPS. The proposed system is based on Equation 5.4 and Equation 5.5 to calculate the distance and angle between two vehicles:

$$Distance = \sqrt{[\,(x_2 - x_1)^2 + (y_2 - y_1)^2]} \tag{5.4}$$

$$Angle = \arctan(y_2 - y_1)\,/(x_2 - x_1) \tag{5.5}$$

where: (x_1, y_1) is the position of the first vehicle and (x_2, y_2) is the position of the second vehicle.

C. Forward Value

The forward value plays an important role in increasing the detection accuracy in self-driving vehicles. The IDS can calculate the forward value of each vehicle; it makes decisions based on the F_v. It is calculated from a trace file that has been generated from ns-2. The IDS considers a vehicle to be malicious when the vehicle does not forward a received packet to the destination after a particular time (T) and forward value (F_v) will be increased by one unit. In other words, it will increase by one-every time an an abnormal behaviour is observed. The F_v is notified to all neighbour vehicles and they update their stored value with the latest. The proposed system considers behaviour of vehicles as normal when the F_v is higher than the threshold such as three otherwise the system will consider abnormal.

D. Assumption

Cooperative Awareness Messages reflect the condition of the surrounding environment and status messages of other vehicles that have joined the platoon. The status messages contain important information such as curvature, position, speed, acceleration, weather, ID, and more. In VANETs communication, each self-driving vehicle acts as a router and host. Hence a vehicle may be the source vehicle at time $t=0$ to generate CAMs. The same vehicle can function as destination to receive packets sent at time $t=n$. that the packets may have been generated from other source vehicles and other intermediate vehicles between source and destination like relay vehicles.

Some rules are established to receive the CAMs otherwise they will be discarded. These rules make the performance of the proposed security system more efficient in terms of detection rate by reducing the number of false alarms and making more efficient use of network resources, such as bandwidth. These rules are [231]:

1. The current CAM must differ by at least four degrees in value of heading from the previous messages or
2. The current CAM must differ by at least 4m in position from the previous message or
3. The current CAM must differ by at least 0.5m/s in speed from the previous message or
4. The current CAM must differ by at least 1s in time from the previous message.

To avoid channel congestion and increase amount of dropped packets, these rules have to be checked every 100ms [152] [232].

E. Communication Area

A self-driving vehicle that wants to communicate with RSUs or vehicles must be in cluster mode. In a clustering scheme, we can find just one vehicle selected as CH based on the TDMA. When another self-driving vehicle joins a cluster area, the group must select one vehicle as CH to manage the group and control transfer of data between multiple vehicles, and also between vehicles and RSUs. The success of this proposal depends on the existing cooperation between CMs and CHs, and this cooperation should be within the coverage area. In other words, the vehicles and CHs should be under the transmission range (Tr) that helps to report abnormal behaviour from vehicles to CH in that zone. The area of vehicle is calculated based on Equation 5.6 [230]:

$$Area\ (Vr) = \mathrm{Tr}\ (\mathrm{Vr}) - \mathrm{T}\ (S_{max} - S_{min}) \tag{5.6}$$

where,

T_r (V_r) is the transmission range of self-driving vehicle Vr.

T is the packet latency in vehicles.

S_{max} is the maximum vehicle speed.

S_{min} is the minimum speed of vehicles.

The proposed IDS algorithm relies on the following basic principles:

1. Malicious vehicles drop or duplicate the data or control that has been received from other surrounding vehicles. These vehicles try to create congestion in the network.
2. While a normal self-driving vehicle forwards packets that have been received to the right destination.

5.4.2 Time Division Multiple Access (TDMA)

F. Intelligent Clustering-IDS

In the clustering scheme, IDS is configured on each self-driving vehicle. The role of CMs is to collect and sniff information of neighbour vehicles in the zone. It is assumed that CHs are trusted in external communication of self-driving vehicles. Each vehicle uses rules and threshold to detect abnormal behaviour when identifying a malicious vehicle. Whether Sybil or wormhole attack; the vehicle will send a message to notify its CH. The CH will block and broadcast malicious IDs to its CMs and to other CHs. Following are the seven stages of the proposed IDS, and the overall architecture of the proposed security system is shown in Figure 5.12.

1. Generate the highway mobility - in this stage, two tools are utilised to generate highway mobility and traffic to simulate the real environment of self-driving vehicles. The output files of this stage are considered input files to ns-2 to generate trace file and routing table of normal and abnormal behaviour.
2. Network Simulator two - CMs will sniff information from other vehicles. They can generate a routing table for each vehicle. Each vehicle will broadcast 3-10 packets/second [233]. The CMs can extract features like timestamp, vehicle ID, GPS position and number of hops from routing table and trace file.
3. Distance and angle calculation - in this stage, the proposed system can calculate distance and angle between vehicles based on values of x-axis and y-axis obtained from GPS and implementing Equation 5.4 and Equation 5.5.
4. Detection phase - in this stage, the IDS on CMs has the ability to detect the wormhole attacks from parameters that have been extracted from the routing table and trace file. The parameters are: the number of hops, forward value and time. The IDS on CMs can identify the Sybil vehicles from normal

vehicles based on some important features, such as distance, angle and vehicle ID.

5. CMs - the IDS on CMs will send notification to CH when it detects a malicious behaviour. It sends a warning message with full details about the malicious vehicle that is detected in clustering mode.
6. Reaction of CHs - the CH will generate alarms and blocks the malicious vehicle to alert other vehicles in inter-clustering. It sends the same warning message to all CHs and RSUs in that zone.
7. Performance metrics - in this stage, we need to evaluate the proposed IDS by calculating the performance metrics such as the packet delay rate, PDR and throughput.

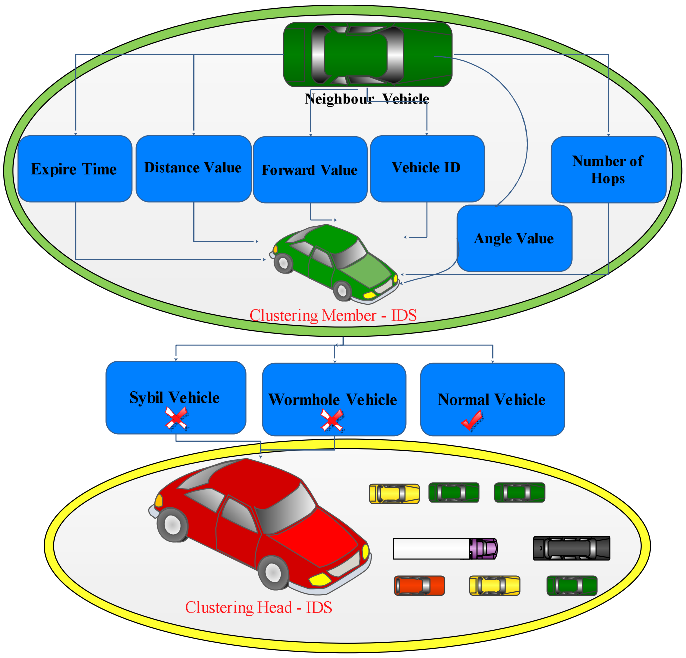


Figure 5.12 IDS Architecture.

As shown in Figure 5.12, the proposed system has six parameters as input to CMs while it has three outputs: malicious vehicle (Sybil / wormhole) and normal vehicle.

G. Simulation Results and Analysis

The proposed IDS can detect two of the most common but serious attacks in VANETs: Sybil and wormhole attacks. Each of these attacks has a different behaviour. Thus, each attack has different parameters to detect malicious behaviour. Figure 5.13 shows type parameters of proposed IDS.

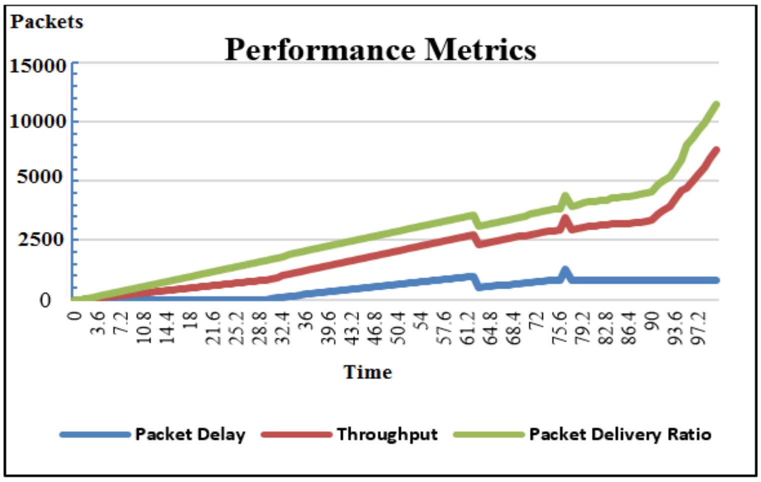


Figure 5.13 Type Parameters of Detection Method.

Here, the performance of proposed IDS needs to be evaluated by analysing efficiency, effectiveness, and calculating the performance metrics. First, Table 5.10 is generated, and it describes the different parameter values that have been extracted, calculated and stored by each vehicle.

Table 5.10 Some Extracted and Calculated Parameters.

Time	Parameters	V_1	V_2	V_3	V_4	V_2
T_0	**Vehicle -ID**	**V_0**	**V_1**	**$V_{wormhole}$**	**V_5**	**V_{9_Sybil}**
	Distance Value	64.6m	97.7m	130m	67.2m	97.7m
	Angle Value	-50.6°	-30.7°	-21°	-48.01°	-30.7°
	Time Stamp	7s	7s	7s	7s	7s
	Forward Value	1	3	2	1	3
	Number of hops	1	2	1	3	2
T_1	**Vehicle –ID**	**$V_{wormhole}$**	**V_1**	**V_4**	**V_5**	**V_{8_Sybil}**
	Distance Value	86.8 m	139.2 m	139 m	107.3 m	139.2 m
	Angle Value	-35.1°	- 21.03°	-21°	-27.7°	-21.03°
	Time Stamp	10s	10s	10s	10s	10s
	Forward Value	1	5	3	11	5

	Number of hops	1	3	5	3	3
T_2	**Vehicle –ID**	**V_0**	**V_1**	**V_4**	**V_5**	**V_{6_Sybil}**
	Distance Value	126.3 m	139 m	139.2	111.8 m	139 m
	Angle Value	-23.3°	-21°	-21°	-26.5°	-21°
	Time Stamp	16s	16s	16s	16s	16s
	Forward Value	1	10	8	12	8
	Number of hops	1	2	3	5	4

Table 5.10 demonstrates the sample database of vehicles that has been collected and calculated from the routing table and trace file. According to Table 5.10, the Sybil attacks are detected by using distance and angle. To detect the wormhole, attack the forward value and number of hops are used.

The average classification rate is collected of two types of attacks targeting self-driving vehicles in VANETs. Our findings are given in Table 5.11:

Table 5.11 Classification Rate of Clustering-IDS.

	Accuracy	Class
IDS - Clustering	72.05%	Normal
	92.2%	Abnormal

The efficiency of the proposed IDS is assessed using ns-2 under two conditions: self-driving vehicles with IDS and self-driving vehicles without IDS. To evaluate the efficiency of VANET with IDS, different performance metrics are calculated, such as PDR, packet delay and throughput [234], as shown in Figure 5.14:

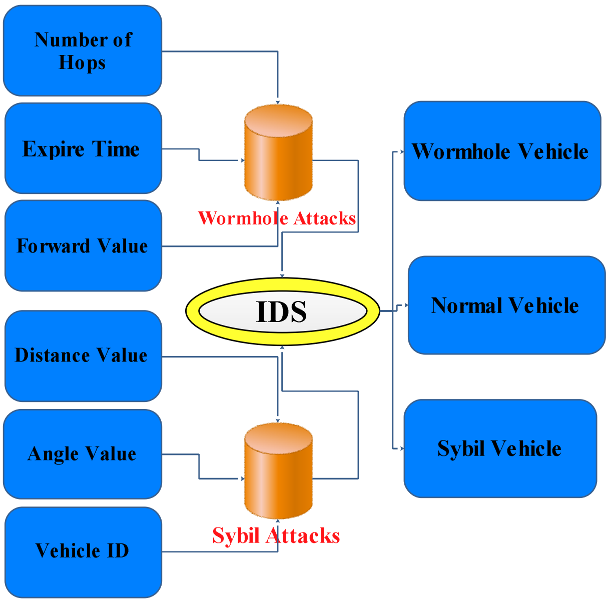


Figure 5.14 Performance Metrics of IDS-Clustering.

A vital role of the proposed IDS is noticed in enhancing the performance of external communication in self-driving vehicles. The proposed system can fix one of the common security problems, which is the lack of fixed security infrastructures; by using the clustering mode in VANETs, a virtual gateway of control built on data and information between vehicles and RSUs.

5.5 System Analysis

Conventional security systems need to be modified in order to provide efficient functionality in protecting these types of VANET networks. The proposed IDS can protect self-driving and semi-self-driving vehicles by detecting malicious vehicles in its external communications. The proposed IDS is mainly suitable for dropping attacks that target broadcasting packets. The intelligent security system is implemented in seven phases: extracting fuzzy parameters, normalisation and fuzzification, rules, apply FPN, prediction phase, training phase and testing phase.

Figure 5.15 illustrates the role of the security system in protecting packets that are sent or received between vehicles in that zone.

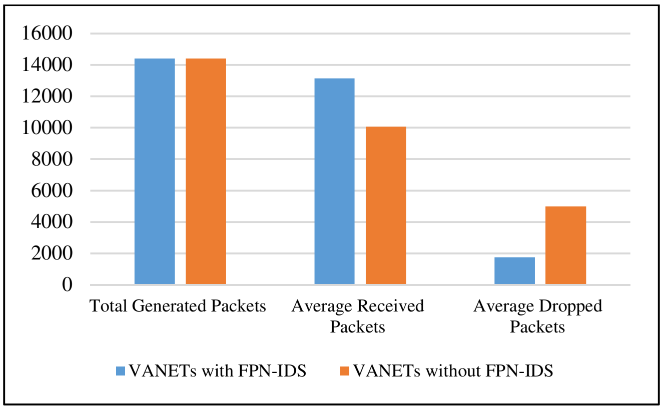


Figure 5.15 Performance Metrics for FPN-IDS.

Artificial intelligence plays a vital role in optimising performance for most scientific projects [235]. Figure 5.15 reflects the vital role of FPN-IDS in enhancing the security of VANETs. It is evaluated under two different conditions: normal and abnormal. The total number of generated packets is 14402 in the two scenarios; the average number of received packets is 13138 of VANETs with IDS and average dropped packets is 1754. However, the average number of received packets is 10064 and average dropped packets is 4982 in VANETs without FPN-IDS. It shows the vital role of the proposed FPN-IDS in external communication of self-driving vehicles. The output metrics explain the range of abnormal behaviour between 0.368 and 0.25.

This security system is compared with a recent research [119] and it is concluded that the scheme provides optimum performance for false positive rate and detection rate. The simulation obtains 0% false positive rate as compared to the rival scheme, which has a false positive rate of 1.6%. The scheme has a 100% detection rate with a 0.42 threshold value, whereas the rival system does not provide an exact measure of the detection rate [119].

According to the experiment, the author can prove the differences between the proportion of detection and false alarms are directly related to a threshold value. However, the use of FPN-IDS enhances the detection rate, whereas decreasing the number of false alarms. Thus, FPN has a direct and positive impact on the result by increasing the detection rate, and decreasing the false alarm rate and error rate. The proposed security system can be extended to design other IDS which can identify and isolate other types of intruders, such as flooding, black hole and grey hole attacks.

The designed response system targets packet dropping in VANETs. By incorporating the response system, the packet delivery rate is improved and the end to end delay of the packet is reduced.

The Clustering-IDS can overcome two common problems; some self-driving vehicles have the same angle but different distances and others have the same distance but different angles. If the proposed IDS is just based on these features, it will be confused in detection which would directly have a negative impact on the detection rate and the number of false alarms, as shown in Figure 5.16.

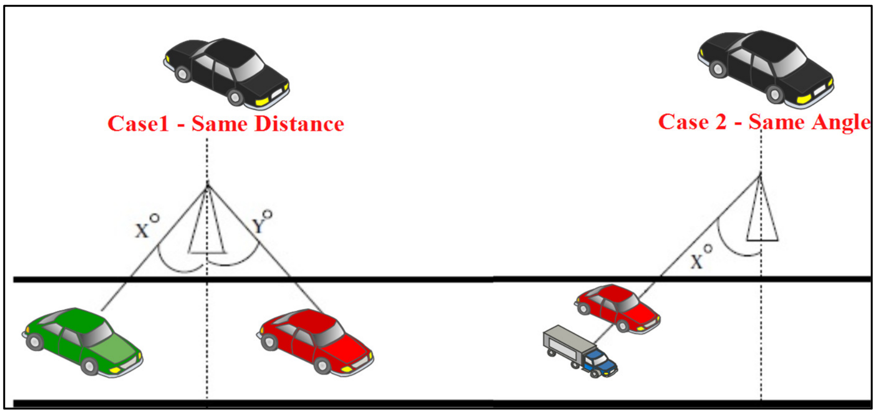


Figure 5.16 Case 1 and Case 2 of Self-Driving Vehicles.

To validate our system, we need to compare our results with other security system such as FPN-IDS [19].

Table 5.12 Classification Rate of IDS.

IDS	Accuracy	Class
IDS -Clustering	72.05 %	Normal
	92.2%	Abnormal
IDS-FPN	58.33	Normal

	%	
	100%	Abnormal

Regarding Table 5.12, a vital role of the IDS-clustering is noticed in enhancing the detection rate of normal behaviour in self-driving vehicles, while IDS-FPN has better a detection rate than IDS-clustering for abnormal behaviour. In future, we can design clustering FPN to get better detection results of normal and abnormal behaviours.

The design of hierarchical IDS based on the clustering mode enhances the detection rate of the proposed IDS in VANETs. Hence IDS-clustering has a direct and positive impact on the resulting system because of the increase in the detection rate, and decrease in the false alarm rate and error rate. The proposed IDS can be extended to build other IDS which can detect other types of attacks, such as flooding, black hole and grey hole attacks.

Both virtual layer that is design on BusNet and the Trust Third Party (TTP) are integrated to build the security system of autonomous vehicles which is the final product of this research. The integration process will be discussed in detail in chapter six showing how the integrated-IDS will enable the detecting and blocking of various attacks that threaten the communication system of self-driving and semi self-driving vehicles.

5.6 Summary

An anomaly FPN-IDS was proposed in this chapter to secure the external communication system of self-driving vehicles. It is based on the extracted parameters that are calculated from the trace file. The FPN-IDS is considered a novel security system to protect VANETs because this is the first time a FPN was used in the design of a security system for VANETs. A response system has been proposed in this chapter which protects compromised vehicles by ensuring communications that are free from intermediaries. An advantage of doing so is that the proposed system achieves a higher packet delivery rate and also improves the end to end delay.

A new response methodology, a 'safe mode' on the data link layer is designed to introduce the infected vehicles in the safe mode at a suitable time. It can be applied to compromised vehicles in order to mitigate the damage caused by the attack. Under normal circumstances, these vehicles are connected with their surrounding communication infrastructure. The safe mode allows the compromised vehicle to communicate directly with the nearby RSUs without any intermediary. Placing a vehicle into 'safe mode' provides partial isolation so that recuperation can take place.

CHAPTER SIX

INTEGRATED INTRUSION DETECTION SYSTEM FOR IDENTIFYING VARIOUS ATTACKS

"The most incomprehensible thing about the world is that it is comprehensible"

Albert Einstein

In this chapter, an integrated-IDS is proposed to secure the external communication system of vehicles against various potential attacks. It is composed of two security systems: BusNet-IDS and distributed-IDS, which are designed to work together. These security systems are based on three components, namely BusNet/virtual layer information, trace and log files information of ns-2 and Center Database (position information, time and ID). This information helps integrated-IDS to detect various attacks such as Sybil, rushing, flooding, drooping, black hole, impersonation and grey hole attacks.

A hierarchical intrusion detection system is based on BusNet layer to sniff/eavesdrop the information among vehicles and send these messages to the closest RSU. The detection process is based on features that have been extracted from control data and warning messages to distinguish between normal and abnormal behaviours. In this security system, the proposed IDS is configured on each RSU to identify abnormal behaviour for vehicles. This security system has the ability to detect various DoS attacks, such as black hole, grey hole, drooping and flooding attacks. Unfortunately, this system cannot detect some tricky attacks, such as Sybil attack. Therefore, a distributed-IDS is proposed in this chapter to secure self-driving vehicles from Sybil attack.

The distributed-IDS is based on Trust Third Party (TTP), like a central dataset to register the position, time and ID for each vehicle on the roads to detect Sybil attacks. In addition, Sybil attack is a leading cause of many types of other attacks, such as node impersonation and fabrication attacks. In other words, the distributed-IDS can detect/identify Sybil, impersonation and fabrication attacks. The application of this security system requires the following:

- All vehicles must be recorded, and they must have an identification number (ID) in any database of roadside units.
- The database is distributed to all roadside units.
- All roadside units must be wire connected with each other (share the same database).

Designing a robust and reliable security system which can protect the external communication system from various attacks. BusNet-IDS system is integrated with a distributed-IDS to detect various attacks. In other words, integrated-IDS is composed of the BusNet-IDS and the distributed-IDS to secure VANETs from Sybil, rushing, flooding, black hole, impersonation, drooping and grey hole attacks.

The detection method can detect abnormal behaviour with a less false alarm rate as is shown by the experiments with the ns-2. The contribution of this chapter can be summarised in three points:

- Proposing the BusNet-IDS: creating a virtual layer between vehicles and RSUs to sniff information and data that is exchanged between vehicles, and calculate/ extract the features from the collected data. These features will be transferred to the closest RSUs in its radio coverage area.
- Proposing the Distributed-IDS: installed TTP like central dataset to register the position for each vehicle on the roads to detect Sybil attacks. In this case, the proposed system has local and global datasets about all registered vehicles. In this system, a mobile agent is proposed and attached with each vehicle to collect

and send important information to the closest RSUs. In addition, two datasets are established in this system which are: a local dataset on RSU and a global dataset on the TTP. Finally, the detection system heavily depends on sharing dataset between RSU with TTP in identifying normal and abnormal behaviour.

- Proposing Integrated-IDS: it is proposed to detect various attacks, such as rushing, flooding, grey hole, black hole and Sybil attacks. In addition, the proposed integrated system is more efficient, faster, and effective than ordinary IDS.

6.1. Integrated Intelligent Intrusion Detection System

To create a practical and robust system an integrated-IDS been proposed in this chapter. The proposed security system is created by merging two security systems i.e. the BusNet-IDS and the distributed-IDS. The resulting system can detect a range of attacks, such as Sybil, black hole, grey hole, flooding and rushing. In the proposed design, the content of a message is determined by selecting one of two integrated IDS. i.e., BusNet-IDS or distributed-IDS. This section gives the IDS detection process for identifying various attacks as given in Algorithm 6.1.

Algorithm – 6.1 Detection Process for the Proposed Integrated-IDS

```
Input: Stream of received messages (msgs) from vehicles; whether control data, CAMs, Notification or warning messages.
Output of the proposed detection system: normal or abnormal behaviours.
For each received message from vehicles do \\ received at RSUs
    Analyse the content for all received msgs \\ Classification of the received msg is broadcast from Bus or normal vehicles
    If msg content is features detection, then Bus_msg
        Bus_msg \\ the proposed IDS will apply the rules detection to identify the attack type
            If $F_1 > F_3$ and,
                $(F_2 / F_1) \leq \theta$ then: the source vehicle is flooding attack
            Else If $F_5 > x$,
                $F_7 > F_8$ and,
                $(F_6 / F_4) < \theta$ **then**: the source vehicle is drooping attack intentionally
                **Else If** $F_7 < F_8$ then this is congestion drop
                **Else**: normal connection
                **End if**
            **End if**
        **End if**
    **Else**: vehicles msg
    **For** each received msg from vehicles, **do**
        The IDS on RSU will analyse the msg content\\ vehicle number and position
        **If** vehicle number match with database and the same vehicle number has two different positions at time n **then**
            This is malicious vehicle (Sybil)\\ the proposed system will match received number of vehicles with local and global database that are stored on RSU and Trusted Third Party
        **Else**: Normal behaviour
        **End if**
    **End for**
    **If** the IDS detect malicious behaviour, **then**:
        Block and broadcast warning msgs to all vehicles in that radio coverage area
    **Else:** confirm the normal behaviour
    **End if**
**End for**
```

The Algorithm 6.1 describes the principal work of the proposed integrated-IDS. The BusNet-IDS and distributed-IDS are discussed in more details of the individual systems. The detection rules R_s are created from the calculated/extracted features. These rules are considered the backbone of the proposed system in the detection and the classification process, as explain below:

- Flooding vehicle is detected in the VANETs if rules (R_1 *and* R_2) hold:

  R_1: if $F_1 > F_3$ and,

  R_2 : $(F_2 / F_1) \leq \theta$ then the source vehicle is flooding attack.

where threshold θ is 0.85, the R_1 check the number of packets generated. In other words, it will check if the intruder sent packets traffic exceeds the communication traffic or the attacker broadcasts more than communication capacity. On the other hand, R_2 will compare the PDR value with θ value, i.e. if the PDR value is less than the θ value, the source vehicle is flooding attack.

- Intentional dropping vehicle - black hole, grey hole and rushing are detected in VANETs if rules R_3, R_4, and R_5 hold:

  R_3 : if $F_5 > x$,

  R_4: $F_7 > F_8$ and,

  R_5: $(F_6 / F_4) < \theta$ then the source vehicle is drooping attack intentionally.

where threshold x is 15 and the dropped packets number exceeds the threshold value in R_3. The R_4 checks the dropped packets whether is due to intentional or congestion. In addition, the congestion drop happens when the number of received packets at the loss monitor vehicle - intermediate is greater than the θ value; otherwise, it is an intentional drop. The R_5 checks the communication system performance (PDR). When PDR is less than the θ value, and R_3 and R_4 hold, that means dropping attacks happened in the external communication system for self-driving and semi-self-driving vehicles.

- Congestion dropping vehicle is detected in VANETs if rule R_6 hold:

  R_6 : if $F_7 < F_8$ then this is congestion drop.

If the R_6 holds then the security system can detect that the loss monitor vehicle – intermediate has made dropping packets due to congestion.

6.1.1 Intrusion Detection System Based on BusNet Layer

A BusNet-IDS is a hierarchical system that is based on a virtual layer. This layer is established between vehicles and RSUs for sniff communication data between them. In detail, BusNet is the bus vehicles utilised to gather conversion data exchanged between vehicles. It works like a cluster-head to monitor and eavesdrop control data and CAMs of members' cluster, which are self-driving vehicles. Hence, it plays a vital role in transferring this detection data to its closest RSUs on road side.

The BusNet layer is just a virtual mobile skeleton infrastructure that is created using public buses. The proposed security system gathers the routing control messages and data packets transmitted among the vehicles using the bus nodes as the cluster-heads. The bus nodes in this situation will calculate/extract the detection features from the original network behaviour information; and these buses will send these extracted features to the closest IDS on the RSUs. When this is done, the road-side unit will be able to see the global view of the vehicular ad hoc networks and it can identify abnormal behaviours by data analysis. It is composed of three layers:

- First layer: vehicle layer
- Second layer: virtual layer
- Third layer: RSU layer

In addition, the structure of these layers is shown in Figure 6.1.

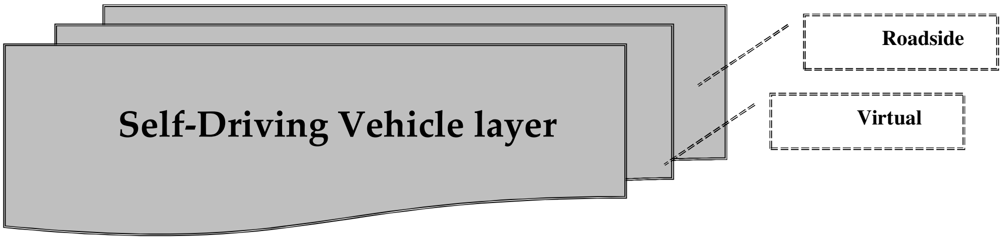


Figure 6.1 Three layers of the Detection System.

Figure 6.2 shows the significant role of BusNet layer in sniffing/eavesdropping data that is transferred/received among moving vehicles and RSUs. However, it can collect data/CAMs, warning messages and notification messages from self-driving vehicles and send it to the closest RSUs.

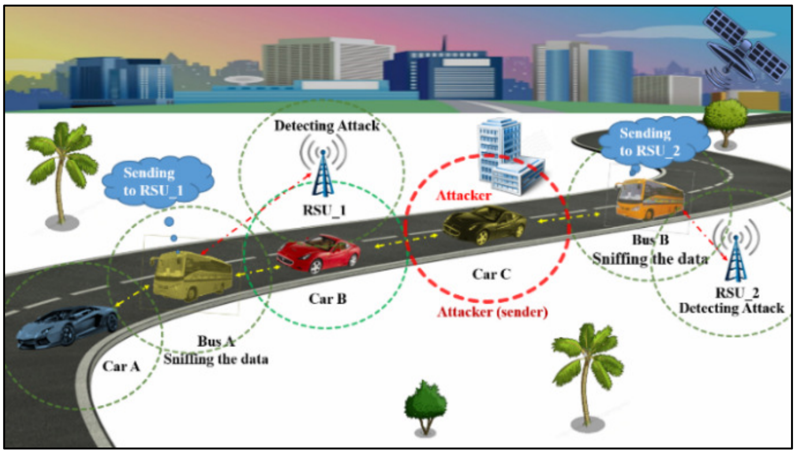


Figure 6.2 BusNet layer Structure.

This security system will solve one of the most significant problems for the wireless channels which is lack of centralised infrastructure. In other words, the BusNet/virtual layer will work like central communication system between vehicles and RSUs.

6.1.1.1 Features Generation

A cluster-based BusNet-IDS is not only able to identify an attack, but also to classify the potential attack types on the VANETs. Various types of features are evaluated by capturing packets from communication systems [236]. In a normal communication behaviour, extracted features are divided into four categories: traffic patterns, network topology, statistics and routing operations [237]. Hence, the proposed security system heavily depends on features vectors that are extracted/ calculated from trace and log files of ns-2.

The trace and log files of ns-2 describe the events of the external communication for autonomous vehicles. It contains many feature vectors which are utilised for analysis. The features describe normal and abnormal behaviours in VANETs. The type and the number of extracted/ calculated features play an important role in the efficient and effective performance of the proposed security system.

6.1. Integrated Intelligent Intrusion Detection System

In general, the statistics are classified into two types, traffic-related and non-traffic-related. The mobility, trace and log files are utilised in calculating the non-traffic-related statistics, such as average route length, route removal count, total route changes and route add count. Whereas the traffic-related statistics are calculated based on trace and log files. In other words, these features involve counting the number of sent, received and forwarded packets between vehicles and RSUs. These features are the number of route reply messages, the number of packets received and the number of packets forwarded [237]. In this chapter, some traffic-related statistics features are calculated/ extracted from the trace and log files of ns-2 that are presented as follows:

- Feature$_{\text{one}}$: it is the number of packets that were transmitted from the source vehicle to the destination vehicle.
- Feature$_{\text{two}}$: it is the number of packets that were received at the destination vehicle from the source vehicle.
- Feature$_{\text{three}}$: it is the maximum number of packets that were received at destination vehicle without drop.
- Feature$_{\text{four}}$: it is the number of packets that were received at the intermediate vehicle – router. These packets are transmitted from the source vehicle to the destination vehicle.
- Feature$_{\text{five}}$: it is the number of packets dropped by the loss monitor vehicle – intermediate that were sent from the source vehicle to the destination vehicle.
- Feature$_{\text{six}}$: it is the number of packets received by the destination vehicle that were forwarded by the loss monitor vehicle.
- Feature$_{\text{seven}}$: it is the total number of arriving packets to loss monitor vehicle that were sent from the source vehicle.

- Feature$_{\text{\_eight}}$: it is the maximum number of received packets at the destination vehicle that were forwarded by the loss monitor vehicle.

The BusNet vehicles are only responsible for calculating features rather than capturing every vehicle's communication features. This is considered a unique aspect of the proposed BusNet-IDS that makes it a robust and reliable system. Besides, the overall performance communication of self-driving vehicles is noticeably better, reducing traffic overhead and burden on VANETs.

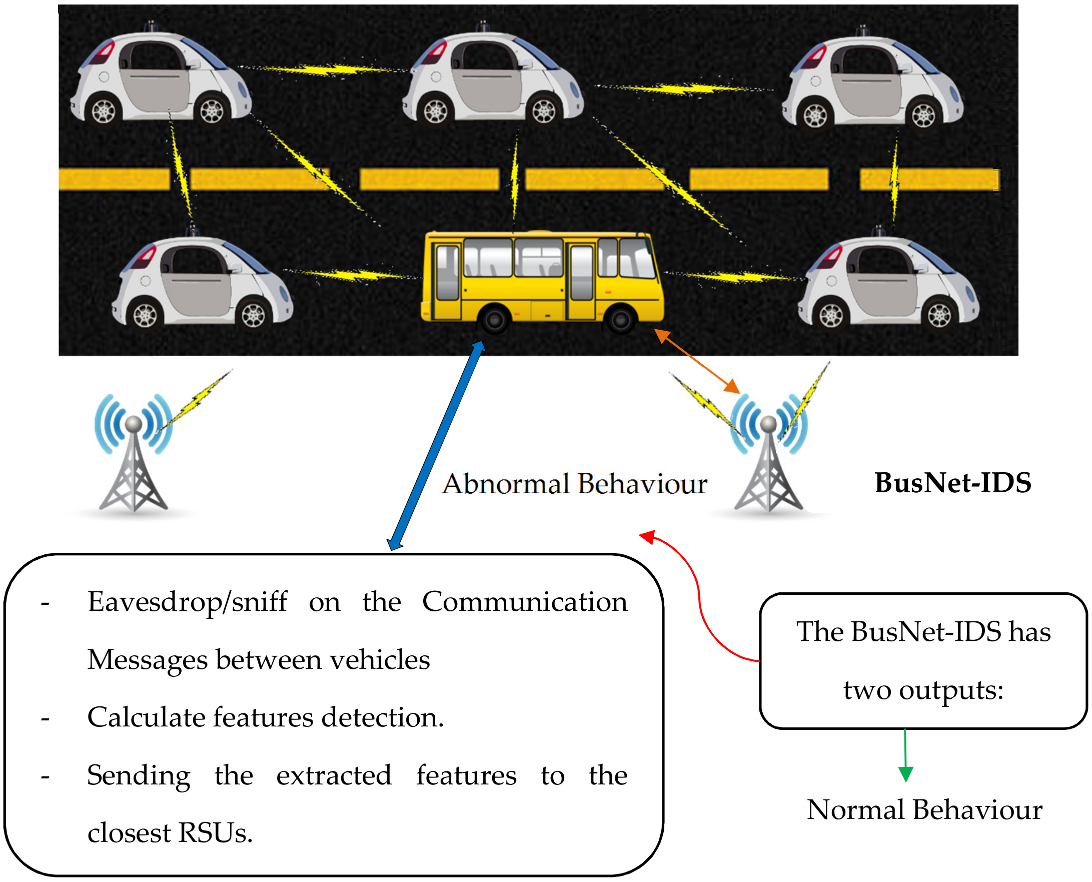
6.1.1.2 Detection Rules

In BusNet-IDS, the detection rules are formulated to detect various attacks on the communication system for self-driving vehicles. In other words, the proposed IDS in the detection process is mainly based on these generated detection rules. The system is composed of features F_n where $n \in \mathbb{N}$ and $1 \leq n \leq 8$. These features will help the proposed IDS to distinguishing between normal and abnormal behaviour. In addition, it has the ability to classify the malicious behaviour into categories, such as flooding and drooping attacks.

In the previous chapters, the proposed IDSs only have the ability to detect the intentional drop because the optimal communication environment is supposed to be in the external communication of self-driving vehicles. In other words, we assume that autonomous vehicles can communicate with high bandwidth channel without congestion. However, the proposed IDS in this chapter has the ability to classify between intentional and congestion dropping. Hence, it can adopt with all communication circumstance.

6.1.1.3 BusNet-IDS Architecture

A hierarchical proposed IDS involves three layers of architecture and IDSs integrated with all RSUs. A novel security system is proposed in this chapter that utilised a virtual layer to protect the sensitive information and control data for self-driving vehicles from the potential attacks. The detection rules of the BusNet-IDS are designed on features vectors that described communication behaviours among vehicles. These features are calculated/ extracted from the routing protocol packages. In other words, IDS heavily depends on features vectors that have been extracted from trace and log files on its detection process, such as rrouter.tcl, trace.tr and rtable.tcl files. Figure 6.3 shows the BusNet-IDS structure.



- Eavesdrop/sniff on the Communication Messages between vehicles
- Calculate features detection.
- Sending the extracted features to the closest RSUs.

Figure 6.3 Proposed BusNet-based Intrusion Detection System.

The role of virtual layer/bus vehicles is to sniff, calculate and send features detection from the exchange information and control data between vehicles to the closest RSUs that were designed with BusNet-IDS. The extracted/calculated features are part from the virtual layer on the bus vehicles. It has the ability to calculate communication features from the behaviour's, whereas, the detection rules are configured with the proposed BusNet-IDSs that were designed on all RSUs. These rules are considered the backbone to the security system created to identify the potential attacks. Hence, these features are utilised in the detection phase for IDS.

The normal and abnormal behaviours are output in detection phase for IDS. In this phase, the extracted features will be matched and compared with the detection rules that were pre-defined for normal behaviour to detect the malicious behaviour. In addition, the security should detect/identify any attack that plays a direct and negative role on communication vehicles of autonomous vehicles.

6.2 Distributed-IDS to Detect Sybil Attacks Based on the Dynamic Position of Vehicles

The major function of VANETs is the provision of improved safety and security for passengers, drivers and vehicles. The open wireless communication medium encouraged intruders to lunch various attacks, including Sybil. This attack on the external communication of self-driving can cause serious damage to the safety and privacy of passengers and drivers in many ways. The Sybil attacks target the accurate location and position information in self-driving vehicles. Hence, this attack can lead to serious life threats.

Position-based information dissemination and location information are considered a critical issue for VANETs in autonomous vehicles, and essentially all safety applications [238]. In addition, this information plays a direct and important role on the precision of collision avoidance, CAMs, notification messages and control data.

A Sybil attack is composed of broadcasting multiple fake identities with false information to break/defeat the strength or trust of an existing communication system [239]. The detection process of a malicious vehicles location becomes a difficult task when Sybil attacks are launched in the external communication system for self-driving vehicles [239]. The Sybil is one of the discussed attacks and is studied owing to the following reasons [59]:

- Sybil attack is a leading cause of many types of other attacks such as node impersonation and fabrication Attacks.
- This kind of attacks is intended to target safety applications in VANETs.
- Sybil attacks vehicular networks: this attack makes identifying or distinguishing the malicious vehicle location very difficult.
- Temporal and spatial constraints make detection Sybil's attacks in VANETs a difficult issue.
- This attack has the ability to defeat the redundancy mechanisms of distributed systems [240].
- Most privacy-preserving schemes are vulnerable to Sybil's attacks.
- This attack has a negative impact on all aspects of network such as network topologies connection, network bandwidth, consumption and human life [59].

The Sybil attacks have two common aspects of the attacks on the communication of the vehicles are [241]:

1. Sybil attack: in this case, the attacker will be on the side of the road and an illusion of a congestion on a road by sending multi-cooperative awareness messages to vehicles with fake IDs or pseudonyms.
2. Denying Existence of a Congestion: this type of attack aims to obscure real congestion for the rest the vehicles, which increases the seriousness of the situation.

This chapter focuses on the detection of various attacks in distributed-IDS. A novel use distributed-IDS is proposed to identify Sybil attack in communication system. The security system is heavily based on local and global datasets that were collected from moving vehicles. In other words, a mobile agent is proposed and attached with each communication system of vehicle to collect and send the detection database to the closest RSUs which are: vehicle ID, time and position information. The distributed database on each RSU is connected with a global database that was saved on the Trusted Third Party.

To deal with transmissions of false information, there are mainly two schemes which are: a trust-based scheme and data-centric scheme [108]. In trust-based scheme, centralised and decentralised infrastructures have been adopted to identify false information [242], [243]. Unfortunately, this scheme cannot detect the false emergency information when it comes from a trusted source [108]. Misbehaviour detection approaches have been proposed to identify malicious behaviour in vehicular networks that were based on data-centric technique [244], [243].

In this chapter, a distributed-IDS is proposed to secure the external communication system that is based on a data-centric scheme. The Distributed-IDS will be designed on RSUs to detect Sybil and impersonation attacks on VANETs. This proposed IDS can differentiate between normal and abnormal (Sybil, impersonation and fabrication) behaviour of vehicles in the network. The security system determines this using local and global databases of vehicles' positions and their associated identification. If an abnormal behaviour is detected, then the ID of the attacking vehicle is broadcast to nearby vehicles and RSU. Figure 6.4 illustrates the basic infrastructures and the scenarios of the IDS to detect Sybil and impersonation attacks. The application of this proposed security system has the following requirements.

- All vehicles must be recorded and there must be an identification number (ID) in any database of the RSUs.
- The database is distributed to all RSUs.
- All RSUs must be connected to each other (share the same central database).

The connection with the VANET cannot be established in situations where a vehicle ID is not registered with the RSU.

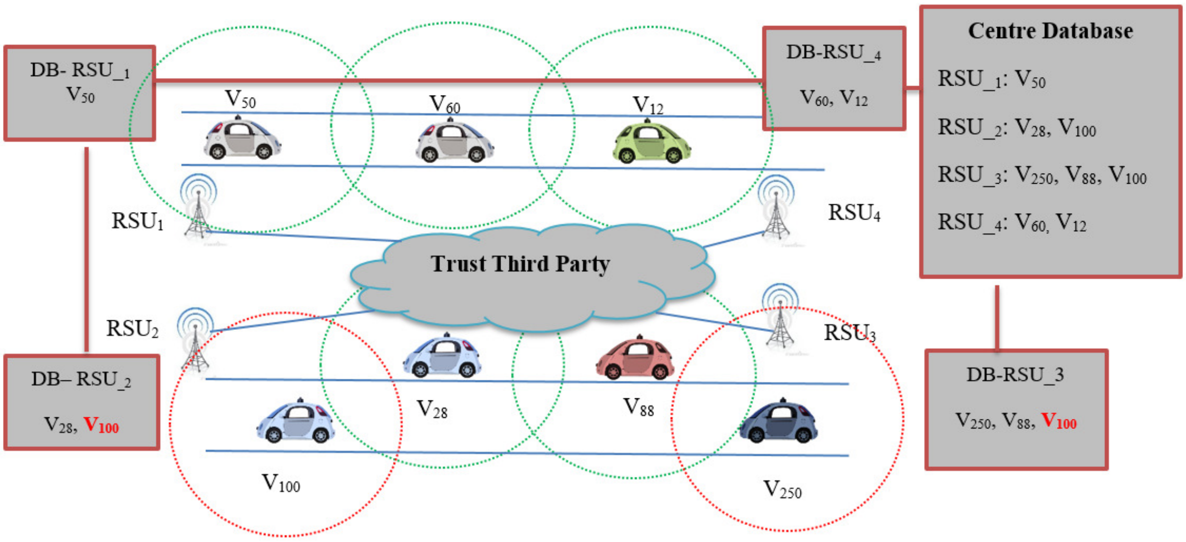


Figure 6.4 Scenarios for the distributed-IDS.

A Sybil attack scenario in figure 6.4 consists of the TTP is node_0, RSUs are nodes (1,2,3, and 4) with wireless communication range of 600m and moving vehicles are remaining nodes within a communication range of 250m.

The Sybil Scenario:

- Vehicle ID_no. 250 has updated its position to RSU_3.
- Vehicle ID_no. 88 has sent a message to vehicle ID_no. 250.
- The message issued by vehicle ID_n.88 will be compared to the database of vehicle ID_no. 250. The RSU provides a new database to vehicle ID_no. 250 and the intrusion detection system in vehicle ID_no. 250 will be verified from the position of the vehicle.
- In this situation, it is detected that the number of this vehicle is in another area so a message is issued to all other vehicles that this vehicle is malicious and will be blocked/isolated.

- Vehicle ID_no. 28 has updated its position to RSU_ 2.
- In this case, it is detected that the number of this vehicle is in another area, issuing a message to all vehicles that this vehicle is malicious and the vehicle is isolated.
- Vehicle ID_no. 3 has updated its position on the roadside unit number 3.
- In case the vehicle is not recorded in roadside units, they cannot connect with VANETs.
- The status of database for RSUs will change dynamically with the movement of vehicles.
- The vehicles must update the status of location depending on their movement.

This attacker can attack by sending a fake number of CAMs with different IDs and pseudonyms to other vehicles, which creates an unreal image of the traffic of vehicles. This generates a kind of confusion in traffic, leading to a lot of accidents. For the detection of malignant vehicles, all vehicles should be recorded in roadside units. These roadside units are maintained by a trusted third party (government), and they are spreaded along the road. In this approach, RSUs will change and share traffic information about the existing vehicles with TTP in that radio coverage area. When the vehicle enters a new area, a new connection should be established with the roadside units. The roadside units will provide the TTP with a message carrying ID for all existing vehicles in the area. The sample of vehicles information shown in table 6.1 that is collected from RSU1, RSU2, RSU3 and RSU4 s:

Table 6.1 Sample of Vehicles Information

RSU_1			
Time/sec	**ID**	**Position**	
		X axis	Y axis
60	0	277.33	313.35

60	2	226.82	313.35
65	0	313.35	198.10
65	2	301.12	313.35
70	2	280.64	316.64
70	4	316.64	194.23
75	1	160.50	313.35
75	2	201.52	316.64
75	4	316.64	290.88
80	1	279.50	313.35
	RSU_$_{2}$		
30	1	178.77	13.35
35	1	285.33	13.35
40	1	308.16	13.35
45	1	308.09	16.64
50	1	262.99	16.64
55	1	176.92	16.64
60	3	253.01	13.35
60	4	243.84	10.05
60	5	197.41	10.05
65	3	304.85	13.35
	RSU_$_{3}$		
0	21	10.05	300.84
0	22	10.05	300.84
0	23	10.05	300.84
120	18	16.64	184.57
120	27	13.34	165.89
120	28	10.05	238.66
120	29	10.05	238.66
120	30	13.33	282.33
120	31	10.05	300.84
120	32	10.05	300.84

RSU_$_4$			
85	18	13.34	144.95
90	0	29.16	16.64
90	3	21.56	16.64
90	7	13.35	25.31
105	2	13.35	89.60
105	3	21.56	16.64
105	14	85.58	13.35
105	23	13.34	141.61
110	0	29.07	16.64
110	2	13.35	69.07

The detection process of distributed-IDS is heavily based on shared database that are mentioned in Table 6.1. In more details, the position, time and ID of vehicles play an important role in detecting and blocking Sybil attacks.

6.3 Integrated-IDS Design and Methodology

The proposed security system provides safety and security environment for the communication system in self-driving vehicles. The proposed systems will work together to detect various attacks that were mentioned above. In general, the road side communication stations will handle different notifications, warnings, cooperative awareness messages from moving vehicles in their respective radio coverage area. In this proposed security system, the content of a received message is specified by choosing one of two the integrated IDS i.e. Distributed-IDS or BusNet-IDS. The steps below explain the methodology that follows in designing this security system.

- Step_$_{\text{one}}$ - Creating mobility and traffic model: in this step, SUMO and MOve software are employed in generating Manhattan mobility and traffic scenarios for self-driving and bus vehicles. The output files from this step will be associated with ns-2 in the step two.

- Step_$_{\text{two}}$ - Establishing communication environment: the communication scenario for vehicles is configured based on ns-2. In addition, all moving vehicles whether vehicles or buses are connected with RSU, as well as establish a TTP. In this scenario, all RSUs are connected by wire with the TTP. The output files of ns-2 reflect all communication behaviours between vehicles and with RSUs. The proposed BusNet-IDS system is based on features that have been extracted from trace file of ns-2. Whereas the distributed-IDS is based on local and global database (share database) that are collected from moving vehicles behaviour, as shown in Figure 6.5.

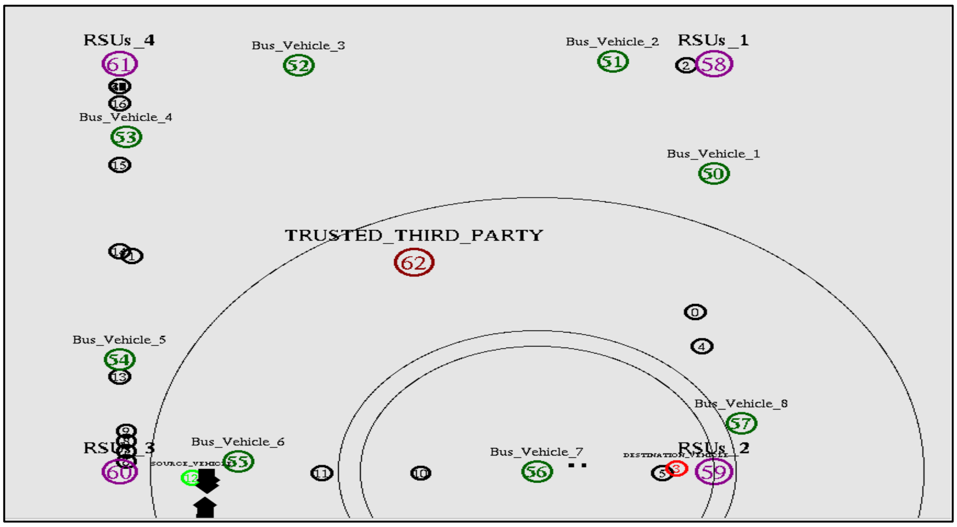


Figure 6.5 Mobility and Traffic scenario.

- Step_$_{\text{three}}$ – Creating select condition for IDS: the content of a received message is determined by selecting one of two integrated IDS i.e. BusNet-IDS or Distributed-IDS. In other words, if the message is composed of feature behaviour obtained from the virtual layer of the Bus vehicle, then it is forwarded to the BusNet IDS. Whereas, if the message contains a vehicle axial positions, time and ID then the message is analysed by the distributed-IDS.

- Step_$_{\text{four}}$ - Designing BusNet layer: this layer is a virtual mobile backbone infrastructure that is built utilising bus vehicles. In other words, mobility nodes work as cluster-heads to sniff/ collect the CAMs, beacons, warning messages and routing control data that were transmitted/ sent between vehicles in radio coverage area. This layer has the ability to transmit the VANETs behaviour information to the closest RSUs. In addition, this virtual layer has the ability to calculate features connection between vehicles. The features that reflect normal behaviour are extracted/calculated from trace files that were collected from the BusNet layer. The detection system relies on features that were described as normal behaviour for vehicles. For example, normal behaviour means that the time interval between two beacon transmissions is 0.4 sec, the payload size of packets is 512B and CBR is traffic application. These vehicles are responsible for sending the extracted features that were mentioned above.
- Step_$_{\text{fifth}}$ – Designing BusNet_IDS: in this IDS, the detection rules are formulated to detect various attacks that were based the extracted features. In other words, the proposed BusNet-IDS in the detection process mainly based on these generated detection rules. The system is composed of features F_n where $n \in \mathbb{N}$ and $1 \leq n \leq 8$. These features will help the proposed security system to distinguish between normal and abnormal behaviours. In addition, it has the ability to classify the malicious behaviour into categories such as: flooding and drooping attacks. The performance of the BusNet-IDS is evaluated in the experimental results to measure the detection rate, false alarm and error rate.
- Step_$_{\text{six}}$: Designing Distributed_IDS: the IDS is heavily based on local and global databases/ shared database that were collected from moving vehicles. In more details, a mobile agent is proposed and attached with

each communication system of vehicles to collect and send the detection database to the closest RSUs, which are vehicle ID, time and position information. The distributed database on each RSU is connected and shared with a global database that was saved on the TTP.

The overall architecture of the proposed Integrated-IDS is shown in Figure 6.6.

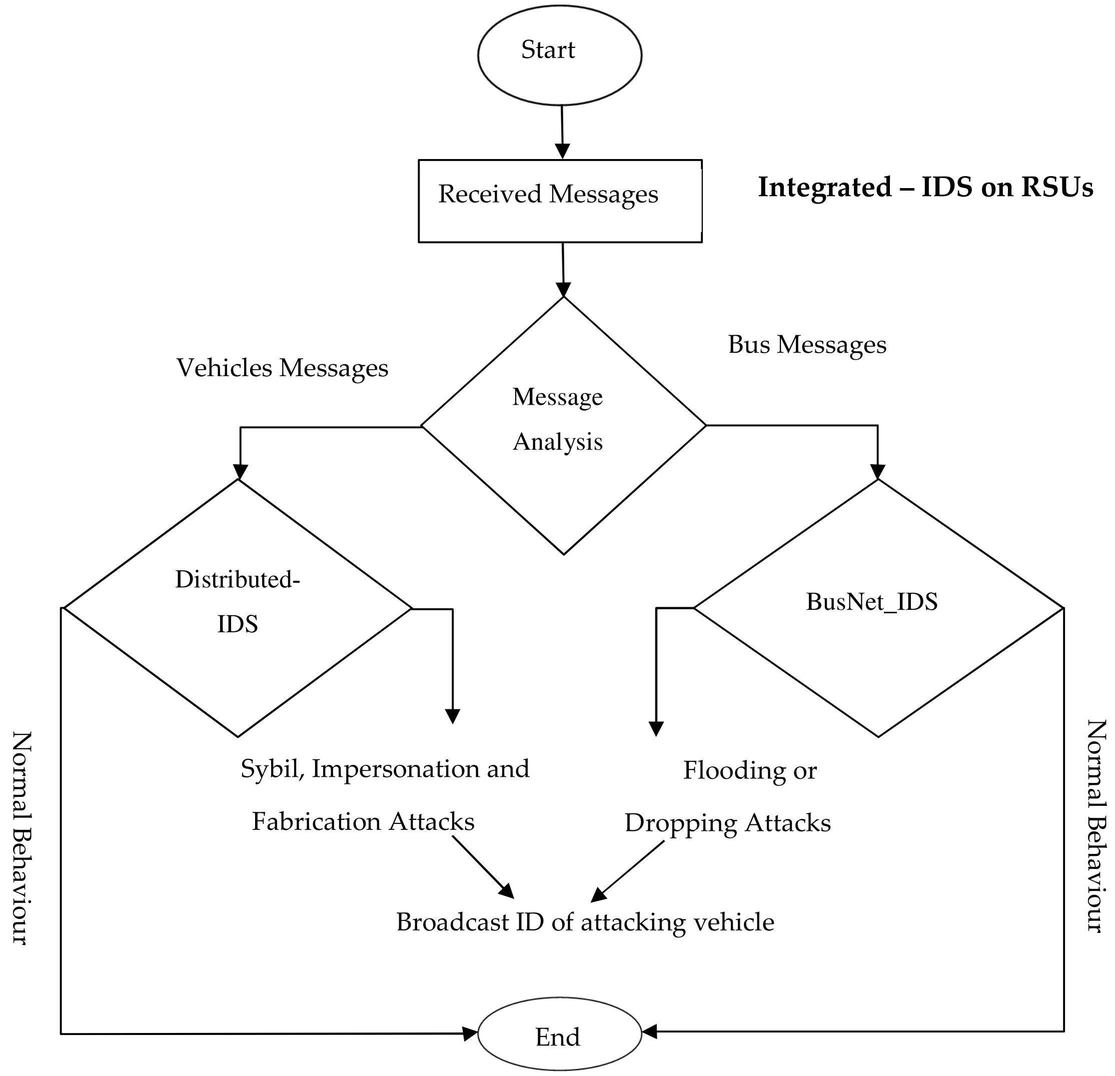


Figure 6.6 Integrated-IDS Flowchart.

Shown in Figure 6.1 is the Integrated-IDS aims to detect various types of attacks using a combination of a distributed-IDS and BusNet IDS. Traffic messages are received by the IDS placed in the RSU. The messages are analysed for vehicle ID, time, position and feature behaviour. In other words, the proposed IDS is heavily based on information that have been extracted from trace, rtable, rrouter files of ns-2.

If the message is composed of feature behaviour obtained from the virtual layer of the Bus vehicle then it is forwarded to the BusNet IDS. This IDS will distinguish between normal and abnormal (flooding or dropping) behaviours of vehicles. If an abnormal behaviour is detected then the ID of the attacking vehicle is broadcast to nearby vehicles and RSU.

If the message contains a vehicle ID and axial positions then the message is analysed by the distributed-IDS. This IDS can differentiate between normal and abnormal (Sybil, impersonation and fabrication) behaviours of vehicles in the network. The IDS determine this using local and global database of vehicles' positions and their associated identification. If an abnormal behaviour is detected, then the ID of the attacking vehicle is broadcast to nearby vehicles and RSU.

6.4 Experiment Simulation

The proposed integrated-IDS was implemented on an ns-2 network simulator platform. It has a simulation area of 600m *600m with a number of vehicles ranging from 20 to 500. In Table 6.2, some of the parameters used in simulating VANETs are: Constant Bit Rate (CBR) application that sends constant packets through a transport protocol such as (UDP or TCP), and Radio Propagation Model (Two Ray Ground) [98].

Table 6.2 Simulator Environmental and Parameters.

Parameter	Value
Simulator	ns-2.35
Simulation time	450*s*
Number of nodes	500 Vehicles
Number of RSUs	4 RSUs
Type of Traffic	Constant Bit Rate (CBR)
Topology	600 x 600 (*m*)
Transport Protocol	UDP- TCP

Packet Size	512
Routing Protocol	V-AODV
Channel type	Wireless
Queue Length	50 packets
Number of Road Lanes	4
Radio Propagation Model	Two Ray Ground
MAC protocol	IEEE 802.11p
Speed	40 m/s
Interface queue type	Priority Queue
Network Interface type	Physical Wireless
Mobility Models	Manhattan Mobility Model

The initial parameters are one of the important issues in ns-2 because they play a vital role in specifying the performance, mobility, traffic type and behaviour of vehicles that are mentioned in Table 6.2.

To evaluate the detection performance of the proposed integrated-IDS, a malicious behaviour is created, whether flooding, dropping, Sybil attacks, in the external communication of self-driving vehicles. In other words, normal and malicious behaviours are generated in the scenario of the proposed IDS to evaluate its detection performance. The abnormal behaviour was established in the ns-2 utilising the OTCL script and OOP. In these scenarios, some files are required to modify/update in V-AODV of VANETs routing protocol. In this thesis, a V-AODV routing protocol is utilised in designing the proposed security system that was mentioned in details in chapter two. The DoS - Flooding is designed to bring connection down by sending/ generating large amounts of traffic that cause a halted connection between vehicles. Whereas DoS - Dropping attack drops received packets rather than forwarding them to the destination vehicle in that radio coverage area. In this section, the performance of integrated-IDS is evaluated under normal and abnormal behaviour.

6.4.1 BusNet-IDS Evaluation

Two types of scenarios, normal/ malicious behaviour and ns-2 are required to evaluate/ test the performance of proposed BusNet-IDS. These behaviours are simulated under certain conditions in order to reflect the efficiency and effectiveness of the security system. The virtual layers that were configured on Bus vehicles will calculate and send the significant features periodically to IDS on the closest RSU. In addition, a criterion is required to measure the efficiency of the proposed security system, and to clarify its role in improving the performance of the external communication systems. The proposed evaluation criteria are detection rate, PDR, false alarms and error rate [211].

Table 6.3 Performance Metrics of BusNet-IDS.

Time/sec	PDR Value	Detection Status
35.0	69.23%	**Congestion**
40.0	87.09%	**Normal**
45.0	90.69%	**Normal**
50.0	93.33%	**Normal**
55.0	22.49%	**Drooping – vehicle 6**
60.0	21.74%	**Drooping – vehicle 6**
65.0	19.66%	**Drooping – vehicle 6**
70.0	21.06%	**Drooping – vehicle 6**
75.0	89.79%	**Normal**
80.0	60.65%	**Congestion**
85.0	64.23%	**Congestion**
90.0	97.15%	**Normal**
95.0	98%	**Normal**
100.0	80.32%	**Normal**
105.0	90.72%	**Normal**
110.0	92.41%	**Normal**
115.0	92.02%	**Normal**
120.0	21.27%	**Dropping – vehicle 42**
125.0	19.29%	**Dropping – vehicle 42**
130.0	20.22%	**Dropping – vehicle 42**

135.0	16.95%	**Dropping – vehicle 42**
140.0	95.04%	**Normal**
145.0	95.85%	**Normal**
150.0	72.19%	**Congestion**
155.0	0.212%	**Flooding – vehicle 31**
160.0	0.190%	**Flooding – vehicle 31**
165.0	0.197%	**Flooding – vehicle 31**
170.0	0.183%	**Flooding – vehicle 31**
175.0	18.82%	**Flooding – vehicle 7**
180.0	17.43%	**Flooding – vehicle 7**
185.0	19.17%	**Flooding – vehicle 7**
190.0	14.01%	**Flooding – vehicle 7**
195.0	78.68%	**Congestion**
200.0	90.06%	**Normal**
205.0	91.46%	**Normal**
210.0	91.36%	**Normal**
215.0	22.49%	**Flooding – vehicle 6**
220.0	21.74%	**Flooding – vehicle 6**
225.0	19.66%	**Flooding – vehicle 6**
230.0	21.06%	**Flooding – vehicle 6**

These metrics are required to approve the detection efficiency of the proposed IDS. The normal, dropping, flooding and congestion behaviour are output result of the proposed IDS that are described in table 6.3. The average of detection rate is 95.85% in our security system.

Table 6.4 shows the detection rate, error rate, TN and FP alarms that are generated in the detection phase of the IDS and it also shows the role of the threshold value and its impact on the accuracy of detection rate. These alarms are calculated by equations 3.5 and 3.7 that were mentioned in chapter three.

Table 6.4 Performance Metrics with False Alarm of BusNet-IDS.

Class	**Average Detection Rate**	**Average Error Rate**
Abnormal behaviour	97.42%	2.58%

Alarm Rate & Threshold – Flooding Attack

Threshold	True Negative	False Positive
0.0	100%	0.0%
0.1	0.0%	100%
0.2	0.0%	100%
0.3	0.0%	100%
0.4	100%	0.0%
0.5	100%	0.0%
0.6	100%	0.0%
0.7	100%	0.0%
0.8	100%	0.0%
0.9	100%	0.0%
1.0	100%	0.0%
Alarm Rate & Threshold – Dropping Attack		
0.0	100%	0.0%
0.1	0.0%	100%
0.80	0.0%	100%
0.81	0.0%	100%
0.82	100%	0.0%
0.83	100%	0.0%
0.84	100%	0.0%
0.85	100%	0.0%
0.86	100%	0.0%
0.87	100%	0.0%
0.88	100%	0.0%
0.89	100%	0.0%
0.9	100%	0.0%
1.0	100%	0.0%

In Table 6.4, the BusNet-IDS can achieve the significant security improvement on the communication system of self-driving vehicles under Flooding and Dropping attacks with an average error rate 2.58%. This IDS has been formally presented in a research paper which was been submitted to EST Conference Kent 2017, United Kingdom, 20-21 September 2017.

6.4.2 Distributed-IDS Evaluation

The detection process in this approach is heavily based on sharing information of RSUs and TTP. This IDS is tested under normal and abnormal behaviours to assess its role in identifying any malicious behaviour. In the detection phase, the collected information of vehicles is employed for testing the ability of the IDS in identifying the malicious behaviour in the external communication system of self-driving vehicles. Table 6.5 shows the accuracy of performance detection, TN, FP and error rate of the proposed distributed-IDS. These metrics reflect the efficient and effective performance of the distributed-IDS that were calculated in Table 6.5.

Overhead rate of communication, messages and update location are required to measure the detection efficiency. The communication overhead is calculated for the proposed distributed-IDS to measure the efficiency of the communication system for self-driving vehicles. In more details, communication-overhead, messages-overhead and location update-overhead are calculated of the communication system for the self-driving vehicles as shown in table 6.6. These values of overhead rate are associated with the number of attacks on the communication system of vehicles.

Table 6.5 Performance Metrics of distributed-IDS.

Class	**Detection Rate**	**Error Rate**
Abnormal behaviour	98%	2.0%
Alarm Rate with Attack Number		
Attack Number	True Negative	False Positive
1	100%	0.0%
3	100%	0.0%
4	99%	1.0%
5	99%	1.0%
6	98%	2.0%
7	98%	2.0%

The calculating process of the overhead values based on equations 6.1, 6.2 and 6.3:

$$Messages - overhead \ = \ CAM \ traffic \qquad (6.1)$$

6.4.2 Distributed-IDS Evaluation

$$Location - overhead \ = \ Location\ traffic \qquad (6.2)$$

$$Communication\text{-}overhead = \quad CAM\ traffic + Location\ traffic \qquad (6.3)$$

where, CAM is cooperative awareness messages that are exchanged between vehicles and RSUs. If the value of the value of field four ($4) equal agent "AGT" and value of file one ($1) of trace file equal send event "s" and value of field seven ($7) equal "CAM" then:

Increase CAM traffic by one ~ CAM ++;

Or

If value of field four ($4) equal "AGT", value of filed one ($1) equal send event "s" and value of field seven ($7) equal "cbr" of trace file equal then:

Increase location traffic by one ~ location traffic++.

Table 6.6 shows the overhead rate for communication, messages and update location.

Table 6.6 Overhead Rate for Communication, Messages and Update Location.

Attacks Number	Communication -Overhead (packets)	Messages-Overhead (packets)	Location Update-Overhead (packets)
1	7497	92	7405
4	7507	102	7405
6	7516	111	7405
8	7525	120	7405
10	7534	129	7405

Whereas, the amount of detection time shown in Table 6.7 that are associated with attacks number on the VANETs.

Table 6.7 Detection Time of distributed-IDS.

Number of Attack	Detection Time/sec
3	$173.45*10^{-3}$
4	$293.766*10^{-3}$
5	$293.766*10^{-3}$
6	$306.7*10^{-3}$
7	$306.7*10^{-3}$

According to the results in Table 6.5, 6.6 and 6.7, we can notice the distributed-IDS based on information of TTP and RSUs has the ability to detect and block one of serious attacks on the external communication system which is Sybil attack. This IDS was formally presented in a research paper which has been submitted at for PLOS Journal 2017.

6.5 System Analysis

The simulation results and analysis of the detection performance of integrated-IDS are covered in this subsection. The average of the detection rate of the integrated-IDS is 97.71% and the average error rate is 2.29%. In order to present an understanding of integrated-IDS in experiment results, the performance analysis has been divided into two subsections as BusNet-IDS and distributed-IDS. The traffic messages are forwarded to suitable IDS whether BusNet-IDS or distributed-IDS that was based on messages contents. In more details, if the message is composed of a feature behaviour obtained from the virtual layer of the Bus vehicle, then it is forwarded to the BusNet IDS. Whereas if the messages contain vehicle ID, time and axial positions, then the message is analysed by the distributed-IDS. In this simulation scenario, trace file, rtable and rrouter files are generated of ns-2 to reflect clear statues of vehicles behaviour.

6.5 System Analysis

Performance metrics are introduced and which have been employed in the previous research. These metrics utilised the efficiency and effectiveness of the IDS. The evaluation metrics utilised in assessing the performance of security system are: PDR, communication overhead, flooding rate, dropping rate, error rate, false alarms and detection time.

In Table 6.3 and 6.4, the BusNet-IDS can achieve the significant security improvement on the communication system of self-driving vehicles under flooding and dropping attacks with an average error rate 2.58%.

The threshold value plays an important role in enhancing the detection rate and reducing the amount of false alarms [119], [223]. To select the optimal value of threshold, the BusNet-IDS is tested with different values of threshold to calculate the accuracy of detection rate and false positive alarm. In this system, the threshold value is set at 0.85 because the most suitable threshold of certainty level lies between 0.4 and 0.99 for Flooding attacks, whereas the most suitable threshold of certainty level lies between 0.82 and 0.99 for dropping attacks. The rate of detection with different thresholds is shown in Figure 6.7.

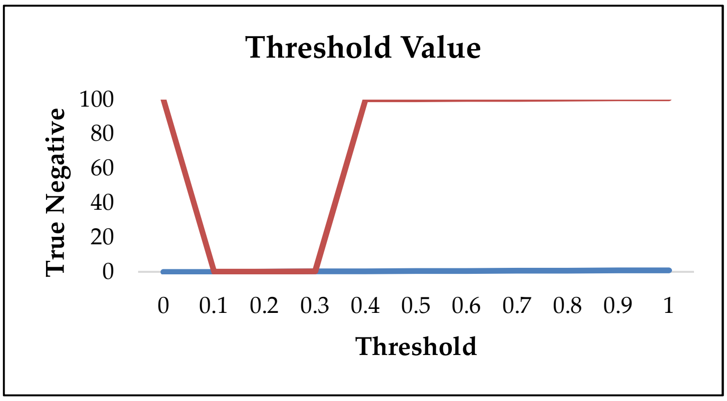


Figure 6.7 Threshold Value.

According to the results in Tables 6.5, 6.6 and 6.7, we can notice distributed-IDS based on information of TTP and RSUs has the ability to detect and block one of serious attacks on the external communication system which is Sybil attack. The detection time and error rate confirm the efficiency of the Distributed-IDS in identifying abnormal behaviour on VANETs.

The feasibility of the application of integrated intrusion detection system is explained below.

1. This security system can detect all external and internal attacks, i.e. common types of DoS attacks such as Dropping and Flooding attacks.
2. The detection system is able to detect all messages that have a fake ID or pseudonym such as Sybil and Impersonation attacks.
3. This mechanism enables us to apply an intrusion detection system of the signature type (misuse). This type is characterised by high precision because errors are not acceptable in self-driving vehicles (low false positives).
4. The system ensures that vehicles can communicate with RSUs directly, without the need for intermediate vehicles.
5. The proposed system has the ability to detect new or novel attacks on wireless communication systems in self-driving vehicles without being predefined for normal or abnormal behaviours.

According to the experimental results, the performance detection of integrated-IDS is faster, more efficient and effective than others because it does not require a training and testing time. Finally, employing integrated-IDS in the external communication system make self-driving and semi-autonomous vehicles more realistic and reliable.

Chapter seven reflects on the overall design and function of the security system introduced in this study. In addition, an outlook on its future application on autonomous vehicles will also be discussed showing its importance to the development of self-driving and semi self-driving vehicles.

6.6 Summary

In this chapter, an efficient intrusion detection system is proposed based on integrating two different intrusion detection systems for the security of the external communication system for self-driving vehicles. It is based on detection rules that were formulated on RSUs with a shared database that reflects communication behaviour for moving vehicles. A novel distributed-IDS and BusNet-IDS are integrated to identify various attacks from the wireless communication system of self-driving vehicles.

The virtual layer is created between mobile vehicles and RSUs to sniff / eavesdrop on exchanged information and control data. This layer is designed on Bus vehicles that extracted the detection features from the warning, notification and CAMs. However, it plays an important role in extracting and sending these features to the closest RSUs.

The distributed-IDS proposed in this chapter identifies Sybil, impersonation and fabrication attacks. It is heavily based on local and global-TTPs database to detect and block any fake ID that was received from moving vehicles. In other words, it matches and compares between received vehicle information and the shared database that was already received and updated with moving vehicles on roads.

CHAPTER SEVEN

CONCLUSION AND FUTURE DIRECTIONS

"The future is much like the present, only longer."

Dan Quisenberry

Self-driving and semi-self-driving vehicles are a recent innovation in the field of automotive research. A hurdle in the wide adoption of this new class of vehicles is security concerns. This research studies the design and implementation of intelligent IDSs to protect the external communication systems in self-driving and semi-self-driving vehicles. The proposed security systems are based on two types of detection approach i.e. anomaly and misuse. The main motivation behind designing the two types of detection approach is to overcome the problems associated with these types of vehicles, such as the lack of accuracy, inability to detect novel attacks, difficulty in updating the database, and increased number of false alarms.

This chapter brings to light novel contributions presented in the thesis. It points out the advantages of the proposed IDS's to protect the external communication for self-driving vehicles. Core contributions are mentioned for each chapter to clarify the role of the proposed security systems that have great positive impact on the self-driving vehicles. The chapter then discusses possible venues for future research.

7.1 Summary of Conclusions

Intelligent intrusion detection systems will have important security applications in many modern technologies, like where they use self-driving and semi-self-driving vehicles [245]. Among many factors the success of self-driving vehicles depends heavily on the integrity of their communication systems. The communication system of self-driving vehicles is often exposed to many different types of attack which impact the development and deployment of self-driving vehicles. Below are the important findings of this research:

Chapter Two presents an in-depth study on the communication system of self-driving vehicles in normal and adversarial environments. It is predicted that more than 250 million autonomous vehicles will be connected to RSUs in the next five years [246]. With one in five vehicles having communication wirelessly by 2020 as well as these vehicles fleets is of growing importance [247], self-driving and semi-self-driving vehicles will be one of many integrated elements in the Internet of Things (IoT). Many security solutions have been proposed that secure VANETs from potential attacks. The following conclusions are drawn from the study of the state of the art

Autonomous and semi-autonomous vehicles use communication systems to exchange warning messages, notification messages, control data and sensitive information. At this point, the security of VANETs is crucial and very important for the development and deployment of self-driving vehicles. VANETs can provide safety to self-driving and semi-self-driving vehicles through cooperative awareness messages and control data which are exchanged between the vehicles and the RSUs within the radio coverage area.

Attempts have been made to secure ad hoc routing protocol [248], [249], [250], [251], [252], [253], [254], [253] and [255]. The routeing protocols cannot completely eliminate all forms of insider attacks. This is due to the fact that intruders are already inside the network with required credentials. A compromised mobility node has all the vital cryptographic keys and can launch several types of attacks, for instance grey hole attacks, routeing loop attacks, and black hole attacks. Hence, it is important to develop detection and response techniques for the external communication of self-driving vehicles.

The V-AODV is a modified version of the original AODV often used in MANETs. In the proposed protocol, algorithm selection is built on determining the optimal communication link between source and destination vehicle. In other words, the algorithm can measure all route weights for the available paths and also select the link with the least communication weight. Thus, the algorithm is a new version of AODV which offers efficient functioning in VANETs. Finally, it is noticed from the experimental results that the proposed V-AODV is more capable of adapting with VANETs with a high packet delivery rate and low end to-end delay.

In Chapter Three, designs of three IDS, which work with ANN and SVM machine learning algorithms, have been presented. They have the ability to detect various types of attacks such as black hole, grey hole and rushing attacks. The IDSs are based on lightweight features that have been extracted from vehicles behaviours. The proposed security system is tested with different dataset to validate the intelligent detection performance. Experimental results show that by building an IDS using ANN and SVM ensures robustness against adversarial manipulation.

The proposed hybrid “anomaly and misuse” IDS has demonstrated a good detection rate with a low rate of false alarms. The proposed IDS plays an important role in identifying and blocking various types of attacks on the VANETs. The hybrid IDS can identify one or more types of DoS attacks which have direct and negative impact on passengers and drivers’ lives as well as sensitive information. Designing a hybrid detection method allows the system to detect new attacks without the high rate of false alarms, improved detection accuracy and update database.

The selection of appropriate lightweight and significant features from vehicle behaviour that describe inter and intra communication between vehicles and their RSUs is a big challenge. The process of decreasing the number of the extracted features by POS scheme has a vital role in enhancing the detection rate.

The fuzzification of dataset help reduce the error rate and the number of false alarms when compared with the previously studied systems. This process is employed to solve some classification problems in dataset which are generated from vehicle behaviours (both normal or abnormal). The normalisation, and uniform distribution techniques are employed in the pre-processing phase. These techniques play an important role in enhancing the detection rate and reducing the number of false alarms.

The proposed intelligent IDS has been evaluated by using Kyoto benchmark dataset. This dataset assists in verifying the efficiency and effectiveness of detection performance in securing the external communication system of self-driving vehicles. In addition, Kyoto-IDS can be used to validate the role of the POS method and fuzzification model in improving the detection rate and reducing false alarms.

In Chapter Four, the traditional IDS is combined with the ICMetric technology to achieve a robust security system for the external communication system of self-driving vehicles called ICMetric-IDS. The ICMetric technology uses the features of a device to create an ICMetric basis number. The number is generated using unique features and characteristics of a device. Suitable features must reflect the characteristics of the sensor devices while the extraction and the analysis process should not significantly influence the device performance. Ultrasonic, accelerometer, gyroscope and magnetometer sensors are employed in designing the ICMetric-IDS. The ICMetric generation is an automated process which does not require user intervention. The ICMetric technology has demonstrated the ability to achieve a reliable authentication over traditional security systems which are based on password and identification numbers. It establishes the identity of a vehicle using its behavioural and physical characteristics. It has shown to be able to augment incumbent security technology in order to establish hardened protection.

The proposed ICMetric based IDS can identify and isolate malicious vehicles thus providing protection to the external communication of self-driving vehicles. The IDS based on ICMetric detects malicious behaviour by monitoring the routeing table and tracing the file generated in network simulator. Simulation results show that the

ICMetric technology was efficient in enhancing detection rate. ICMetric-IDS is based on the FFNN algorithm and is efficient, effective and has lower error rate in detecting malicious vehicles than ICMetric-IDS based on k-NN algorithm. The proposed security system achieves significant security improvements on the external communication system of self-driving vehicles under various types of attacks with average error rate 0.72%.

In Chapter Five a framework called FPN-IDS has been proposed. The FPN-IDS is considered a novel security system designed to protect VANETs because this is the first time an FPN has been used in VANETs. The FPN-IDS has the ability to detect external and internal attacks launched at any time such as packet dropping attacks. Anomaly FPN-IDS is based on the parameters that are computed from the trace file. The FPN has a vital role in increasing the detection rate and decreasing false alarms for proposed IDS.

The Clustering-IDS can overcome two common problems which are that some self-driving vehicles have the same angle but different distances and others have the same distance but different angles. A vital role of the IDS-clustering is noticed in enhancing the detection rate of normal behaviour in self-driving vehicles, while IDS-FPN had better detection rate than IDS-clustering. It can provide high levels of security to external communications in self-driving vehicles. In addition, a hierarchical IDS is proposed to detect Sybil and Wormhole attacks by using log records. The design of hierarchical IDS based on clustering mode enhances the detection rate of IDS in VANETs. Hence IDS-clustering has a direct and positive impact on the resulting system because of the increase in the detection rate, decrease in the false alarm and error rate.

The chapter also presents a new response system that is designed to put infected/ compromised vehicles into safe mode at suitable time without delay. The response system is built on the data link layer of the network that switches the infected vehicle from normal operations to a 'safe mode'. The safe mode allows the compromised vehicle to communicate directly with the nearby RSUs without any intermediary. Placing a vehicle into 'safe mode' provides partial isolation so that recuperation can take place.

In Chapter six the design of an integrated intrusion detection system is presented that secures the external commination system of self-driving vehicles from attacks like Sybil, dropping, flooding, DoS, black hole, impersonation and grey hole attacks. The proposed IDS is composed of three components i.e. BusNet layer, trace file and a central database for location information.

BusNet-IDS is simulated and the results show that it is efficient in detecting abnormal behaviours in VANETs. It has the ability to sniff/eavesdrop important information exchanged between vehicles and RSUs. The BusNet-IDS can detect common types of attacks such as DoS, dropping, flooding, rushing, grey hole, black hole and wormhole attacks. The distributed intelligent IDS is proposed in this chapter to detect Sybil and Impersonation attacks. It is able to detect all messages that have a fake ID or pseudonyms. Sharing of database between trusted third party and RSUs supports the detection phase of the proposed security system to enable the detection of one type of tricky attacks on communication system, which is Sybil attack. The proposed integrated-IDS can overcome common detection problems faced with single IDS such as adapting to different behaviours of attacks. In addition, detection process in single IDS is relies on local resources for data collection hence no exchange of data takes place.

7.2 Future Directions

The work proposed in this thesis is an effort to enhance the security of driverless vehicles. It is possible today to purchase a driverless vehicle but the technology is far from perfect. There is room for improvement in all domains related to driverless vehicles. The work presented in this thesis is novel and requires specific infrastructure for successful implementation. To fully implement the proposed system in real life it is necessary that road side units are installed across all national highways. These road side units should be equipped with network and computation capabilities. Besides this every self-driving vehicle should be able to carry out external and internal communications. To ensure security the self-driving vehicle should be embedded with an intelligent system which is able to detect external obstacles, provide security functionalities, make observations using vision system. When these individual systems function collaboratively then the safety and security of the vehicles can be ensured.

Research shows that system defences evolve to address the advancements made by adversaries in their resources and capabilities. Thus, designers of system intrusion prevention systems are always trying to stay one step ahead of adversaries. The proposed work attempts to improve the security of existing systems and also opens up new venues for future research. There are many ways in which the proposed work can be extended.

Efforts have been made to secure the external communications of autonomous vehicles. To secure this unique environment, research needs to be done on the security of the internal communication system of the autonomous vehicles. Doing so would create a robust communication system that can resist both internal and external attacks.

To improve the detection rate while reducing the number of false alarms, a clustering FPN can be designed to get better results in both normal and abnormal behaviours. This security system has the ability to detect various attacks on the communication system of self-driving system. In other words, integrated clustering model with FPN to get robust and new security system.

7.2 Future Directions

The proposed security system can also be tested using other methodologies that employ artificial intelligence. Techniques such as Self-Organising Maps (SOM), Bayesian trees and genetic algorithms can be used to test the security and practicality of autonomous vehicles. Testing and evaluating the proposed security system with another dataset to validate the detection performance.

Research can be done to improve the routeing protocol for VANETs. This can be achieved by using intelligent e-maps to determine vehicle destination. Research should also study the applications and effectiveness of handover mechanisms in VANETs.

It is important to improve road safety, logistics and information services. However, the efficiency and performance of VANET applications depend primarily on the way in which messages are transmitted between the vehicles. Improvement can be made to specific characteristics and constraints of VANET, such as speed, acceleration, geographical position, the transmission radius, management, etc.

Introduction of a central controller with the right communication solution can make processes more efficient, improve provider collaboration, enhance the driver experience and support decision making processes. Speed and quality of signals are the most important part of all process associated with VANET. This means all operations must be arrived at easily, operations with providers directly and find the information they need instantaneously. They expect continuity and simplicity across all points of contact with their central control.

Extracting the ICMetric number from other sensor devices such as LiDAR can be explored. However, comparison between results must be carried out to analyse the performance compared to the proposed ultrasonic and MEMS sensors.

A concept worth exploring is the design of a distribute-IDS that can be configured on vehicles and RSUs simultaneously. This design can be a major improvement as this can improve the functioning of the network entities through the integration of local and global datasets and credentials.

Bibliography

[1] A. M. Wyglinski, X. Huang, T. Padir, L. Lai, T. R. Eisenbarth, and K. Venkatasubramanian, "Security of Autonomous Systems Employing Embedded Computing and Sensors," *IEEE Micro*, vol. 33, no. 1, pp. 80–86, Jan. 2013.

[2] World Health Organization, "Global Status Report on Road Safety," *Injury prevention*, 2015. [Online]. Available: http://www.who.int/violence_injury_prevention/road_safety_status/2015/en/. [Accessed: 10-Apr-2017].

[3] M. Hashem Eiza, "Secure Multi-Constrained QoS Reliable Routing Algorithm for Vehicular Ad hoc Networks (VANETs)," PhD Thesis, Brunel University London, 2014.

[4] Bryant Walker Smith, "Human Error As Cause of Vehicle Crashes," 2013. [Online]. Available: http://cyberlaw.stanford.edu/blog/2013/12/human-error-cause-vehicle-crashes. [Accessed: 13-Mar-2017].

[5] S. Thrun, "Toward robotic cars," *Commun. ACM*, vol. 53, no. 4, p. 99, Apr. 2010.

[6] I. Org, T. A. Litman, and T. Litman, "www.vtpi.org Autonomous Vehicle Implementation Predictions Implications for Transport Planning," *Traffic Technol. Int.*, pp. 36–42, 2014.

[7] M. O. Cherif, "No Optimization of V2V and V2I communications in an operated vehicular network," Doctor of Université de Technologie de Compiègne," France, 2010.

[8] S. K. Gehrig and F. J. Stein, "Dead reckoning and cartography using stereo vision for an autonomous car," in *Proceedings 1999 IEEE/RSJ International Conference on Intelligent Robots and Systems. Human and Environment Friendly Robots with High Intelligence and Emotional Quotients (Cat. No.99CH36289)*, 1999, vol. 3, pp. 1507–1512.

[9] M. Chaudhry, C. Seth, and A. Sharma, "Feasibility Analysis of Driverless Car Using VANETs," *Discovery*, vol. 15, no. 1542, pp. 86–88, 2014.

[10] H. Hasbullah, I. A. Soomro, and J. A. Manan, "Denial of Service (DOS) Attack and Its Possible Solutions in VANET," *Int. J. Electr. Comput. Energ. Electron. Commun. Eng.*, vol. 4, no. 5, pp. 411–415, 2010.

[11] M. Raj and K. Institue, "Routing and Security Analysis in Vehicular Ad-Hoc Networks (VANETs)," in *Power Electronics, Intelligent Control and Energy Systems*

(ICPEICES),IEEE International Conference on, 2016, pp. 1–5.

[12] H. Hartenstein and K. Laberteaux, *VANETs : vehicular applications and inter-networking technologies*. Wiley, 2010.

[13] D. Zelikman and M. Segal, “Reducing Interferences in VANETs,” *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 3, pp. 1582–1587, Jun. 2015.

[14] H. Moustafa and Y. Zhang, *Vehicular networks : techniques, standards, and applications*. CRC Press, 2009.

[15] V. de Cózar, J. Poncela, M. Aguilera, M. Aamir, and B. S. Chowdhry, “Cooperative Vehicle-to-Vehicle Awareness Messages Implementation,” Springer Berlin Heidelberg, 2013, pp. 26–37.

[16] S.-I. Sou, “Modeling Emergency Messaging for Car Accident over Dichotomized Headway Model in Vehicular Ad-hoc Networks,” *IEEE Trans. Commun.*, vol. 61, no. 2, pp. 802–812, Feb. 2013.

[17] A. M. Vegni, M. Biagi, and R. Cusani, “Smart Vehicles, Technologies and Main Applications in Vehicular Ad hoc Networks,” *INTECH Open Access Publ.*, no. ISBN 978-953-51-0992-1, 2013.

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

[19] K. M. A. Alheeti, A. Gruebler, K. D. McDonald-Maier, and A. Fernando, “Prediction of DoS attacks in external communication for self-driving vehicles using a fuzzy petri net model,” in *2016 IEEE International Conference on Consumer Electronics (ICCE)*, 2016, pp. 502–503.

[20] K. M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, “An intrusion detection system against malicious attacks on the communication network of driverless cars,” in *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, 2015, pp. 916–921.

[21] J. Petit and S. E. Shladover, “Potential Cyberattacks on Automated Vehicles, IEEE Transactions on Intelligent Transportation Systems,” vol. 16, no. 2, pp. 1–11, 2015.

[22] D. Tian, Y. Wang, G. Lu, and G. Yu, “A vehicular ad hoc networks intrusion detection system based on BUSNet,” *2010 2nd Int. Conf. Futur. Comput. Commun.*, pp. V1-225-

V1-229, 2010.

[23] N. Garg and P. Rani, “An improved AODV routing protocol for VANET (Vehicular Ad-hoc Network),” vol. 4, no. 6, pp. 1885–1890, 2015.

[24] T. Lomax David Schrank and S. Turner, “Urban Mobility Information,” PhD thesis, The Texas A&M University System, 2015.

[25] M. Kubat, “A Simple Machine-Learning Task,” in *An Introduction to Machine Learning*, Cham: Springer International Publishing, 2015, pp. 1–18.

[26] N. R. C. (US), “Artificial Intelligence Applications to Critical Transportation Issues, Transportation Research Board. Artificial Intelligence and Advanced Computing Committee. TRB. 2012.”

[27] F. Dressler, F. Kargl, J. Ott, O. K. Tonguz, and L. Wischhof, “Research challenges in intervehicular communication: Lessons of the 2010 Dagstuhl seminar,” *IEEE Commun. Mag.*, vol. 49, no. 5, pp. 158–164, 2011.

[28] J. J. Blum, A. Eskandarian, and L. J. Huffman, “Challenges of intervehicle Ad Hoc networks,” *IEEE Trans. Intell. Transp. Syst.*, vol. 5, no. 4, pp. 347–351, 2004.

[29] P. M. Khilar and S. K. Bhoi, “Vehicular communication: a survey,” *IET Networks*, vol. 3, no. 3, pp. 204–217, 2014.

[30] G. Chandrasekaran, “VANETs: The Networking Platform for Future Vechicular Applications,” *PhD Thesis, Rutgers Univ.*, pp. 45–51, 2007.

[31] S. intersections, “National Highway Traffic Safety Administration, Vehicle Safety Communications Project Final Report,” U.S. Dept. of Transportation, 2008.

[32] A. Boukerche, *Algorithms and Protocols for Wireless, Mobile Ad Hoc Networks*, vol. 3. John Wiley & Sons, 2008.

[33] S. Khan and A.-S. Khan Pathan, Eds., *Wireless Networks and Security*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013.

[34] M. Erritali and B. El Ouahidi, “A review and classification of various VANET Intrusion Detection Systems,” *2013 Natl. Secur. Days - 3eme Ed. Des Journees Natl. Secur. JNS3*, 2013.

[35] M. Fiore, J. Harri, F. Filali, and C. Bonnet, “Vehicular Mobility Simulation for VANETs,” in *40th Annual Simulation Symposium (ANSS’07)*, 2007, pp. 301–309.

[36] J. Muller, “No Hands, No Feet: My Unnerving Ride in Google’s Driverless Car,” 2013.

[Online]. Available: www.forbes.com/sites/joannmuller/2013/03/21/%0Ano-hands-no-feet-my-unnerving-ride-in-googlesdriverless-car/%0A. [Accessed: 30-Apr-2013].

[37] N. Highway Traffic Safety Administration and N. Center for Statistics, "TRAFFIC SAFETY FACTS 2010 A Compilation of Motor Vehicle Crash Data from the Fatality Analysis Reporting System and the General Estimates System POLICE-REPORTED MOTOR VEHICLE TRAFFIC CRASHES," 2010.

[38] M. D. Meyer, "CRASHES VS. CONGESTION, What's the Cost to Society?," *American Automobile Association, Heathrow, FL, 2008.* [Online]. Available: http://newsroom.aaa.com/wp-content/uploads/2011/11/2011_AAA_CrashvCongUpd.pdf. [Accessed: 30-Jan-2017].

[39] W. D. U. S. D. of T. N. H. T. S. Administration, "National Motor Vehicle Crash Causation Survey Report to Congress." [Online]. Available: http://www.nrd.nhtsa.dot.gov/ Pubs/811059.PDF. [Accessed: 17-Apr-2013].

[40] J. M. Lutin, A. L. Kornhauser, and E. Lerner-Lam, "The Revolutionary Development of Self- Driving Vehicles and Implications for the," *ITE J.*, no. July, p. 5, 2013.

[41] "Technical Report, How RobotCar works – Oxford Robotics Institute." [Online]. Available: http://www.ori.ox.ac.uk/how-robotcar-works/. [Accessed: 01-Feb-2017].

[42] KPMG, "Self-driving cars: The next revolution A message from Gary Silberg and Richard Wallace, [Accessed: 02-Feb-2017]."

[43] L. Laursen, "Vehicle-to-Vehicle Communications Tech Will Be Mandatory, say Feds," 2014.

[44] S. Shladover, "Recent International Activity in Cooperative Vehicle–Highway Automation Systems Quality Assurance Statement,No. FHWA-HRT-12-033, California PATH (2012, [Accessed: 30-Feb-2017]."

[45] S. R. T. for the Environment, "First demonstration of SARTRE vehicle platooning," 2011. [Online]. Available: http://www.sartre-project.eu/en/press/Documents/Press release 20110117 First_test_platooning doc.pdf. [Accessed: 30-Jan-2017].

[46] "IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," p. i-513, 2003.

[47] "The DSRC Project." [Online]. Available: http://www.leearmstrong.com/-dsrc/dsrchomeset.htm. [Accessed: 17-May-2014].

[48] "IEEE 802.11." [Online]. Available: http://grouper.ieee.org/groups/802/11/. [Accessed: 18-May-2014].

[49] H. Wu, "Analysis and Design of Vehicular Networks," Georgia Institute of Technology, 2005.

[50] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks, Journal of Computer Security," vol. 15, no. 1, pp. 39–68, Jan. 2007.

[51] I. A. Sumra, I. Ahmad, H. Hasbullah, and J. bin Ab Manan, "Classes of attacks in VANET," in *2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC)*, 2011, pp. 1–5.

[52] B. Parno and A. Perrig, "Challenges in securing vehicular networks," *Work. hot Top. networks*, no. 4, pp. 1–6, 2005.

[53] A. M. Malla and R. K. Sahu, "Security Attacks with an Effective Solution for DOS Attacks in VANET," *Int. J. Comput. Appl.*, vol. 66, no. 22, pp. 45–49.

[54] J. R. Douceur, "The Sybil Attack," *Int. Work. Peer-to-Peer Syst. Springer Berlin Heidelb.*, pp. 251–260, Mar. 2002.

[55] X. Feng, C. Li, D. Chen, and J. Tang, "A method for defensing against multi-source Sybil attacks in VANET," *Peer-to-Peer Netw. Appl.*, Jan. 2016.

[56] J. T. Isaac, S. Zeadally, and J. S. Cámara, "Security attacks and solutions for vehicular ad hoc networks," *IET Commun.*, vol. 4, no. 7, p. 894, 2010.

[57] "Take details about internal components for vehicles connect with VANETs." [Online]. Available: http://www.iamatechie.com/time-for-accident-free-roads/5211. [Accessed: 19-May-2014].

[58] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaaniche, and Y. Laarouchi, "Survey on security threats and protection mechanisms in embedded automotive networks," in *2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W)*, 2013, pp. 1–12.

[59] J. M. Shaikh, "A comparative Analysis of Routing Protocols in VANET environment using realistic vehicular traces, PhD Thesis," 2010.

[60] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust

management for Vehicular Networks: An Adversary-Oriented Overview," *IEEE Access*, vol. 4, pp. 1–1, 2016.

[61] Kobayashi, "An integrated mobility and traffic model for vehicular wireless networks," *2nd ACM Int. Work. Veh. ad hoc networks - VANET '05*, pp. 69–78, 2000.

[62] V. Kumar, S. Mishra, and N. Chand, "Applications of VANETs: Present &amp;amp; Future," *Commun. Netw.*, vol. 5, no. 1, pp. 12–15, 2013.

[63] S. Vivek, "Vehicular ad hoc networks," PhD Thesis, Indian Institute of Technology Univ., Kharagpur, 2010.

[64] H. Guo and G. Liu, "Research of security for vehicular ad hoc networks," in *2010 International Conference on Computer, Mechatronics, Control and Electronic Engineering*, 2010, vol. 5, pp. 144–147.

[65] S. Arya and J. Tewari, "Routing Overheads in Vehicular Ad Hoc Networks (VANETs)," *Conf. Adv. Commun. Control Syst.*, vol. 2013, no. Cac2s, pp. 267–270, 2013.

[66] X. Lin, X. Ling, H. Zhu, P.-H. Ho, and X. S. Shen, "A novel localised authentication scheme in IEEE 802.11 based Wireless Mesh Networks," *Int. J. Secur. Networks J. Secur. Networks*, vol. 3, no. 2, pp. 122–132, 2008.

[67] A. Nadeem and M. P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2027–2045, 2013.

[68] R. Heady, G. Luger, A. Maccabe, and M. Servilla, "The Architecture of a Network-Level Intrusion Detection System," *Zhurnal Eksp. i Teor. Fiz.*, vol. 0, 1990.

[69] T. Leinmuller, E. Schoch, and C. Maihofer, "Security requirements and solution concepts in vehicular ad hoc networks," in *2007 Fourth Annual Conference on Wireless on Demand Network Systems and Services*, 2007, pp. 84–91.

[70] O. Pattnaik and B. K. Pattanayak, "Security in Vehicular Ad Hoc Network based on Intrusion Detection System," *Am. J. Appl. Sci.*, vol. 11, no. 2, pp. 337–346, Feb. 2014.

[71] G. Samara, W. a H. Al-Salihy, and R. Sures, "Security issues and challenges of Vehicular Ad Hoc Networks (VANET)," *New Trends Inf. Sci. Serv. Sci. NISS 2010 4th Int. Conf.*, pp. 393–398, 2010.

[72] M. Raya, P. Papadimitratos, and J. Hubaux, "Security Vehicular Communications," *IEEE Wirel. Commun.*, vol. 13, no. 5, pp. 8–15, Oct. 2006.

[73] I. Aad, J.-P. Hubaux, and E. W. Knightly, “Impact of Denial of Service Attacks on Ad Hoc Networks,” *IEEE/ACM Trans. Netw.*, vol. 16, no. 4, pp. 791–802, Aug. 2008.

[74] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, “Vehicular ad hoc networks (VANETS): status, results, and challenges,” *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, Aug. 2012.

[75] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, “Denial of Service Attacks in Wireless Networks: The Case of Jammers,” *IEEE Commun. Surv. Tutorials*, vol. 13, no. 2, pp. 245–257, 2011.

[76] W. Xu, W. Trappe, Y. Zhang, and T. Wood, “The feasibility of launching and detecting jamming attacks in wireless networks,” in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing - MobiHoc ’05*, 2005, p. 46.

[77] G. Karagiannis *et al.*, “Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions,” *IEEE Commun. Surv. Tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[78] X. Lin, R. Lu, C. Zhang, H. Zhu, P. h. Ho, and X. Shen, “Security in vehicular ad hoc networks,” *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 88–95, Apr. 2008.

[79] C. Campolo and A. Molinaro, “Multichannel communications in vehicular Ad Hoc networks: a survey,” *IEEE Commun. Mag.*, vol. 51, no. 5, pp. 158–169, May 2013.

[80] T. M. de Sales, H. O. Almeida, A. Perkusich, L. de Sales, and M. de Sales, “A privacy-preserving authentication and Sybil detection protocol for vehicular ad hoc networks,” in *2014 IEEE International Conference on Consumer Electronics (ICCE)*, 2014, pp. 426–427.

[81] V. K. Tripathi and S. Venkaeswari, “Secure communication with privacy preservation in VANET- using multilingual translation,” in *2015 Global Conference on Communication Technologies (GCCT)*, 2015, pp. 125–127.

[82] M. N. Mejri, J. Ben-Othman, and M. Hamdi, “Survey on VANET security challenges and possible cryptographic solutions,” *Veh. Commun.*, vol. 1, pp. 53–66, 2014.

[83] R. Coussement, B. Amar Bensaber, and I. Biskri, “Decision support protocol for intrusion detection in VANETs,” in *Proceedings of the third ACM international symposium on Design and analysis of intelligent vehicular networks and applications - DIVANet ’13*, 2013, pp. 31–38.

[84] P. Ping Yi, Y. Yichuan Jiang, Y. Yiping Zhong, and S. Shiyong Zhang, "Distributed Intrusion Detection for Mobile Ad Hoc Networks," in *2005 Symposium on Applications and the Internet Workshops (SAINT 2005 Workshops)*, 2005, pp. 94–97.

[85] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," *IEEE Wirel. Commun.*, vol. 11, no. 1, pp. 48–60, Feb. 2004.

[86] R. E. Shannon, *Introduction to the art and science of simulation*. IEEE Computer Society Press, 1998.

[87] A. K. Pandey, "Simulation of Traffic Movement in Vanet Using SUMO," National Insititute of Technology Certificate, NIT Rourkela, 2013.

[88] "The Network Simulator - ns-2." [Online]. Available: http://www.isi.edu/nsnam/ns/. [Accessed: 20-Jun-2016].

[89] R. S. Keshav, "Cornell University; minnie.tuhs.org." [Online]. Available: http://minnie.tuhs.org/PhD/th/8Implementing_TRUMP_RBCC_in.html. [Accessed: 08-Jun-2014].

[90] J. Wang, "ns-2 Tutorial (1)," *Event (London)*, no. 1, pp. 1–16, 2004.

[91] R. Technologies, "No Title"Riverbed application and network performance management solutions." [Online]. Available: http://www.riverbed.com/products/performancemanagement-control/opnet.html. [Accessed: 20-Jun-2016].

[92] Estinet-Technologies, "EstiNet Network Simulator and Emulator," no. September, pp. 110–117, 2013.

[93] S. N. Technologies, "The Communications Simulation Platform QualNetNo Title." [Online]. Available: http://web.scalable-networks.com/content/qualnet. [Accessed: 22-Jun-2016].

[94] "No TitleGlobal Mobile Information System Simulator (GloMoSim)." [Online]. Available: http://pcl.cs.ucla.edu/projects/glomosim/. [Accessed: 23-Jun-2016].

[95] "No TitleJava in Simulation Time / Scalable Wireless Ad hoc Network Simulator (JiST/SWANS)." .

[96] F. Rocha, "NS2 Visual Trace Analyzer, Technical Report," 2010. [Online]. Available: http://www.nsnam.com/2012/10/ns2-visual-trace-analyzer.html. [Accessed: 20-Jun-2014].

[97] T. J. E. Altman, “NS Simulator for beginners,” 2003. [Online]. Available: https://www-sop.inria.fr/members/Eitan.Altman/ns.htm. [Accessed: 15-Jul-2016].

[98] E. H. T. Issariyakul, *Introduction to Network Simulator NS2*. Springer, 2011.

[99] Ns3, “NS2 versus NS3 Comparison between NS2 and NS3,” *I*, p. Retrieved on May 10, 2013 from.

[100] D. Djenouri, W. Soualhi, and E. Nekka, “VANET’s Mobility Models and Overtaking: An Overview,” in *InInformation and Communication Technologies: From Theory to Applications. ICTTA 2008. 3rd International Conference on 2008 Apr 7, IEEE.*, pp. 1–6, 2008.

[101] F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, “CityMob: A Mobility Model Pattern Generator for VANETs,” in *ICC Workshops - 2008 IEEE International Conference on Communications Workshops*, 2008, pp. 370–374.

[102] B. Ramakrishnan, “CBVANET : A Cluster Based Vehicular Adhoc Network Model for Simple Highway Communication,” *Adv. Netw. Appl.*, vol. 761, pp. 755–761, 2011.

[103] F. J. Martinez, J. C. Cano, C. T. Calafate, and P. Manzoni, “CityMob: A mobility model pattern generator for VANETs,” *IEEE Int. Conf. Commun.*, pp. 370–374, 2008.

[104] D. B. Johnson, D. A. Maltz, and J. Broch, “DSR: the dynamic source routing protocol for multihop wireless ad hoc networks,” pp. 139–172, Mar. 2001.

[105] A. Mahajan, “Urban mobility models for vehicular ad hoc networks,” *Second Asian Internet Eng. Conf. AINTEC 2006, Pathumthani, Thailand, Novemb. 28-30, 2006 Proc.*, p. 251, 2006.

[106] M. Chatterjee, “Small-Scale and Large-Scale Routing in Vehicular Ad Hoc Networks,” *IEEE Trans. Veh. Technol.*, vol. 58, no. 9, pp. 5200–5213, Nov. 2009.

[107] D. Helbing, “Traffic and related self-driven many-particle systems,” *Rev. Mod. Phys.*, vol. 73, no. 4, pp. 1067–1141, Dec. 2001.

[108] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, “Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6703–6714, 2016.

[109] D. Huang, S. Misra, M. Verma, and G. Xue, “PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs,” *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 736–746, Sep. 2011.

[110] A. N. Shen, S. Guo, D. Zeng, and M. Guizani, "A lightweight privacy-preserving protocol using chameleon hashing for secure vehicular communications," *IEEE Wirel. Commun. Netw. Conf. WCNC*, pp. 2543–2548, 2012.

[111] Rongxing Lu, Xiaodong Li, T. H. Luan, Xiaohui Liang, and Xuemin Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, Jan. 2012.

[112] R. Lu, X. Lin, H. Zhu, and P, "-H. Ho, and X. Shen, 'ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications,'" *Proc. IEEE INFOCOM'08, Phoenix, AZ, USA, April*, vol. 14, p. 18, 2008.

[113] P. Papadimitratos, A. Kung, J.-P. Hubaux, and F. Kargl, "Privacy and Identity Management for Vehicular Communication Systems: a Position Paper," *Present. Work. Stand. Priv. User-Centric Identity Manag. Zurich, Switz.*, 2006.

[114] H. Sedjelmaci, S. M. Senouci, and M. Feham, "An efficient intrusion detection framework in cluster-based wireless sensor networks," *Secur. Commun. Networks*, vol. 6, no. 10, p. n/a-n/a, Jan. 2013.

[115] J. Petit, M. Feiri, and F. Kargl, "Spoofed data detection in VANETs using dynamic thresholds, in Proceedings of the IEEE Vehicular Networking Conference (VNC 2011), Amsterdam, Netherlands," pp. 25–32, 2011.

[116] N. Bißmeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for VANETs based on mobility data plausibility," *Proc. ACM VANET*, p. 73, 2012.

[117] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking - MobiCom '00*, 2000, pp. 275–283.

[118] J. Rupareliya, S. Vithlani, and C. Gohel, "Securing VANET by Preventing Attacker Node Using Watchdog and Bayesian Network Theory," *Procedia Comput. Sci.*, vol. 79, pp. 649–656, 2016.

[119] A. Chaudhary, V. N. Tiwari, and A. Kumar, "Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks," *Souvenir 2014 IEEE Int. Adv. Comput. Conf. IACC 2014*, pp. 256–261, 2014.

[120] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP &#x2014; Sybil Attacks Detection in Vehicular Ad Hoc Networks," *IEEE J. Sel. Areas Commun.*, vol.

29, no. 3, pp. 582–594, 2011.

[121] W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, 2016.

[122] C. A. Kerrache, A. Lakas, and N. Lagraa, "Detection of Intelligent Malicious and Selfish Nodes in VANET using Threshold Adaptive Control," in *Electronic Devices, Systems and Applications (ICEDSA), 2016 5th International Conference on*.

[123] N. Bißmeyer, C. Stresing, and K. M. Bayarou, "Intrusion detection in VANETs through verification of vehicle movement data, 2010 IEEE Vehicular Networking Conference, VNC 2010," pp. 166–173, 2010.

[124] S. K. Bhoi and P. M. Khilar, "A secure routing protocol for Vehicular Ad Hoc Network to provide ITS services," *2013 Int. Conf. Commun. Signal Process.*, vol. 83, no. 4, pp. 1170–1174, 2013.

[125] A. S. Nadav Schweitzer Ariel Stulman and R. D. Margalit, "Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks," *IEEE Trans. Mob. Comput.*, vol. 1233, no. c, pp. 1–10, 2016.

[126] R. Baiad, H. Otrok, S. Muhaidat, and J. Bentahar, "Cooperative cross layer detection for blackhole attack in VANET-OLSR, IWCMC 2014 - 10th International Wireless Communications and Mobile Computing Conference," pp. 863–868, 2014.

[127] X.-Y. Guo, C.-L. Chen, C.-Q. Gong, and F.-Y. Leu, "A Secure Official Vehicle Communication Protocol for VANET," *2016 10th Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput.*, pp. 482–485, 2016.

[128] M. Nafaa and Y. Ghamri-doudane, "Anomaly-Based Intrusion Detection System for Ad hoc Networks," in *Network of the Future (NOF), 2016 7th International Conference on the*, 2016, pp. 0–2.

[129] M. K. Usha and A. S. Poornima, "Node-to-node authentication protocol to prevent black hole attack in AODV," *Proc. 2016 IEEE Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2016*, pp. 133–136, 2016.

[130] M. Feiri, J. Petit, and F. Kargl, "Efficient and secure storage of private keys for pseudonymous vehicular communication," *First Work. Secur. Priv. Dependability CyberVehicles (CyCar '13) 20th ACM Conf. Comput. Commun. Secur. (CCS '13)*, pp.

9–18, 2013.

[131] S. Dietzel, J. Petit, G. Heijenk, and F. Kargl, “Graph-based metrics for insider attack detection in VANET multihop data dissemination protocols,” *IEEE Trans. Veh. Technol.*, vol. 62, no. 4, pp. 1505–1518, 2013.

[132] M. Nema, S. Stalin, and R. Tiwari, “RSA algorithm based encryption on secure intelligent traffic system for VANET using Wi-Fi IEEE 802.11p,” *IEEE Int. Conf. Comput. Commun. Control. IC4 2015*, pp. 2–6, 2016.

[133] N. Bimeyer, K. H. Schröder, J. Petit, S. Mauthofer, and K. M. Bayarou, “Short paper: Experimental analysis of misbehavior detection and prevention in VANETs,” *IEEE Veh. Netw. Conf. VNC*, pp. 198–201, 2013.

[134] M. Feiri, J. Petit, R. K. Schmidt, and F. Kargl, “The impact of security on cooperative awareness in VANET,” *IEEE Veh. Netw. Conf. VNC*, pp. 127–134, 2013.

[135] R. Tahir, H. Tahir, and K. McDonald-Maier, “Securing Health Sensing Using Integrated Circuit Metric,” *Sensors*, vol. 15, no. 10, pp. 26621–26642, Oct. 2015.

[136] J. Petit, F. Schaub, M. Feiri, and F. Kargl, “Pseudonym Schemes in Vehicular Networks: A Survey,” *IEEE Commun. Surv. Tutorials*, vol. 17, no. 1, pp. 228–255, 2015.

[137] K. Zaidi, M. Rajarajan, S. Furnell, and A. Hudson-Smith, “Vehicular Internet: Security & Privacy Challenges and Opportunities,” *Futur. Internet*, vol. 7, pp. 257–275, 2015.

[138] A.-S. K. Pathan, *Security of Self-Organizing Networks*. Taylor & Francis Group, 2011.

[139] M. Alimohammadi and A. A. Pouyan, “Sybil Attack Detection Using a Low Cost Short Group Signature in VANET,” pp. 23–28, 2015.

[140] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, “Distributed Aggregate Privacy-Preserving Authentication in VANETs,” *IEEE Trans. Intell. Transp. Syst.*, pp. 1–11, 2016.

[141] A. K. Saha and D. B. Johnson, “Modeling Mobility for Vehicular Ad Hoc Networks,” in *in Proceedings of ACM International Workshop on Vehicular Ad Hoc Networks*, 2004, pp. 91–92.

[142] S. Singh and S. Agrawal, “VANET routing protocols: Issues and challenges,” *2014 Recent Adv. Eng. Comput. Sci. RAECS 2014*, pp. 6–8, 2014.

[143] A. K. Ali and I. Phillips, “Evaluating VANET Routing in Urban Environments,” *39th*

Int. Conf. Telecommun. Signal Process., pp. 60–63, 2016.

[144] C. H. Lee, Y. C. Su, and L. G. Chen, “Accurate positioning system based on street view recognition,” *ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc.*, pp. 2305–2308, 2012.

[145] “Oxbotica’s Software For Self-Driving Cars Doesn’t Need GPS Signal | Popular Science.” [Online]. Available: http://www.popsci.com/software-for-self-driving-cars-without-gps. [Accessed: 28-Feb-2017].

[146] P. S. Nithya Darisini and N. S. Kumari, “A survey of routing protocols for VANET in urban scenarios,” in *2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering*, 2013, pp. 464–467.

[147] “How Google’s Self-Driving Car Works,” 2011. [Online]. Available: http://spectrum.ieee.org/automaton/robotics/artificial-intelligence/how-google-self-driving-car-works. [Accessed: 07-Nov-2015].

[148] O. Mahmoud *et al.*, “A feature selection method for classification within functional genomics experiments based on the proportional overlapping score.,” *BMC Bioinformatics*, vol. 15, no. 1, p. 274, Jan. 2014.

[149] J. Ramkumar and R. Murugeswari, “Fuzzy Logic Approach for Detecting Black Hole,” *Int. Jounal Innov. Res. Sci. Eng. Technol.*, vol. 3, no. 3, pp. 877–882, 2014.

[150] K. Lan, “Realistic mobility models for Vehicular Ad hoc Network (VANET) simulations,” in *2008 8th International Conference on ITS Telecommunications*, 2008, pp. 362–366.

[151] W. M. Danquah and D. Turgay Altilar, “HYBRIST Mobility Model -A Novel Hybrid Mobility Model for VANET Simulations,” *Int. J. Comput. Appl.*, vol. 86, no. 14, pp. 975–8887, 2014.

[152] J. Breu, A. Brakemeier, and M. Menth, “Analysis of cooperative awareness message rates in VANETs,” *2013 13th Int. Conf. ITS Telecommun. ITST 2013*, pp. 8–13, 2013.

[153] “Manual interpretation of ns2 trace file,” 2010. [Online]. Available: https://getch.wordpress.com/2010/11/20/manual-interpretation-of-ns2-trace-file/. [Accessed: 09-Aug-2016].

[154] J. G. and D. Dasgupta and Abstract, “Evolving Fuzzy Classifiers for Intrusion Detection Jonatan,” in *Proceedings of the 2002 IEEE Workshop on Information Assurance*, 2002.

[155] "Technical Report, Distributions for assigning random values—Data Management toolbox | ArcGIS Desktop." [Online]. Available: http://pro.arcgis.com/en/pro-app/tool-reference/data-management/distributions-for-assigning-random-values.htm#GUID-90B1E835-3A98-4582-A64E-E6A0D878D92E. [Accessed: 06-Oct-2017].

[156] "Using Artificial Intelligence to create a low cost self-driving car," 2014. [Online]. Available: http://budisteanu.net/Download/ISEF 2 Autonomous car Doc particle.pdf. [Accessed: 12-Jul-2016].

[157] K. D. Thilak and A. Amuthan, "DoS attack on VANET routing and possible defending solutions — A survey," in *2016 International Conference on Information Communication and Embedded Systems (ICICES)*, 2016, pp. 1–7.

[158] K. M. Ali, W. Venus, and M. S. Al Rababaa, "The affect of fuzzification on neural networks intrusion detection system," *2009 4th IEEE Conf. Ind. Electron. Appl. ICIEA 2009*, pp. 1236–1241, 2009.

[159] S. M. Al-Naqshabandi, "Simulation system for computer network intrusion detection," Al-Nahrain University - Baghdad - Iraq, 2007.

[160] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, "Network intrusion detection," *IEEE Netw.*, vol. 8, no. 3, pp. 26–41, May 1994.

[161] "propOverlap: Feature (gene) selection based on the Proportional Overlapping Scores," 2014. [Online]. Available: https://cran.r-project.org/web/packages/propOverlap/index.html. [Accessed: 09-Aug-2016].

[162] O. Mahmoud *et al.*, "A feature selection method for classification within functional genomics experiments based on the proportional overlapping score.," *BMC Bioinformatics*, vol. 15, no. 1, p. 274, Jan. 2014.

[163] H. J. Zimmermann, *Fuzzy set theory and its applications*, no. 3. Kluwer, Boston, 2nd ed., 1993., 1993.

[164] M. Hellmann, *Fuzzy Logic Introduction*, no. 1. University Rennes, 1965.

[165] J. Gomez and D. Dasgupta, "Evolving Fuzzy Classifiers for Intrusion Detection," *Proc. 2002 IEEE Work. Inf. Assur.*, no. June 2001, pp. 1–5, 2002.

[166] K. M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, "An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars," in *2015 Sixth International Conference on Emerging Security Technologies*

(EST), 2015, pp. 86–91.

[167] S. Peddabachigari, A. Abraham, and J. Thomas, "Intrusion Detection System Using Support Vector Machine and Decision Tree," *Int. J. Comput. Appl.*, vol. 3, no. 3, pp. 40–43, 2010.

[168] L. (Eds. . Camps-Valls, G., Bruzzone, *Kernel Methods for remote Sensing Data Analysis*, Section 5. New York, NY, USA: Wiley, 2009.

[169] K. M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, "On the detection of grey hole and rushing attacks in self-driving vehicular networks," in *2015 7th Computer Science and Electronic Engineering Conference (CEEC)*, 2015, pp. 231–236.

[170] K. Ali Alheeti, A. Gruebler, and K. McDonald-Maier, "Intelligent Intrusion Detection of Grey Hole and Rushing Attacks in Self-Driving Vehicular Networks," *Computers*, vol. 5, no. 3, p. 16, Jul. 2016.

[171] D. V. K. MD. Ezaz Ahmed Dr. Y.K. Mathur, "Knowledge Discovery in Health Care Datasets Using Data Mining Tools," *Int. J. Adv. Comput. Sci. Appl.*, vol. 3, no. 4, 2012.

[172] J. Song, H. Takakura, Y. Okabe, M. Eto, D. Inoue, and K. Nakao, "Statistical analysis of honeypot data and building of Kyoto 2006+ dataset for NIDS evaluation," in *Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security - BADGERS '11*, 2011, pp. 29–36.

[173] K. A. and K. McDonal-Maier, "Hybrid Intrusion Detection in Connected Self-Driving Vehicles," in *22nd IEEE International Conference on Automation and Computing (ICAC'16)*, 2016.

[174] S. H. Baek, D.-H. Park, and H. Bozdogan, "Hybrid kernel density estimation for discriminant analysis with information complexity and genetic algorithm," *Knowledge-Based Syst.*, vol. 99, no. March, pp. 79–91, 2016.

[175] K. M. A. Alheeti, A. Gruebler, and K. McDonald-Maier, "Using Discriminant Analysis to Detect Intrusions in External Communication of Self-Driving Vehicles," *Digit. Commun. Networks*, 2017.

[176] "Researcher Hacks Self-driving Car Sensors," 2015. [Online]. Available: http://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors. [Accessed: 15-Oct-2015].

[177] M. Feng, Y. Fukuda, M. Mizuta, and E. Ozer, "Citizen Sensors for SHM: Use of

Accelerometer Data from Smartphones," *Sensors*, vol. 15, no. 2, pp. 2980–2998, 2015.

[178] S. Dey, N. Roy, W. Xu, R. R. Choudhury, and S. Nelakuditi, "AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable, NDSS '14, 23-26 February 2014, San Diego, CA, USA."

[179] A. B. BOJINOV, H., MICHALEVSKY, Y., NAKIBLY, G. and D., *Mobile Device Identification via Sensor Fingerprinting. National Research & Simulation Center, Rafael, arXiv preprint arXiv:* p. 1408.1416, 2014.

[180] K. D. McDonald-Maier, W. G. J. Howells, Y. Kovalchuk, D. Gu, and H. Hu, "A practical proposal for ensuring the provenance of hardware devices and their safe operation," in *7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012*, 2012, pp. 11–11.

[181] "Technical Report, Ultrasonic Ranging Module HC - SR04." [Online]. Available: http://www.micropik.com/PDF/HCSR04.pdf. [Accessed: 25-Oct-2015].

[182] A. Kokosy, M. Pepper, and C. Donzé, "SYSIASS – an intelligent powered wheelchair," 2012.

[183] R. E. Carroll, N. Garraud, J. A. Little, M. J. Mazzoleni, B. P. Mann, and D. P. Arnold, "Investigation of wave propagation phenomena in microfabricated arrays of nonlinearly coupled oscillators," in *2015 Transducers - 2015 18th International Conference on Solid-State Sensors, Actuators and Microsystems (TRANSDUCERS)*, 2015, pp. 1227–1230.

[184] R. Kuc, *Electrical engineering in context: smart devices, robots &amp; communications*. Boston, MA, USA, 2014.

[185] L. Castoldi, "The MEMS Revolution," 2012. [Online]. Available: http://www.semi.org/eu/sites/semi.org/files/docs/STM.pdf. [Accessed: 21-Jul-2016].

[186] "Self-driving cars: The next revolution - 2012." [Online]. Available: https://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/self-driving-cars-next-revolution.pdf.

[187] H. Bojinov, D. Boneh, Y. Michalevsky, and G. Nakibly, "Mobile Device Identification via Sensor Fingerprinting."

[188] D. Xia, C. Yu, and L. Kong, "The development of micromachined gyroscope structure and circuitry technology, Sensors Journal," vol. 14, no. 1, pp. 1394–1473, 2014.

[189] S. Tanaka, “State-of-the-art MEMS Gyroscopes for Autonomous Cars,” in *Twelfth International Conference on Flow Dynamics*, 2015, pp. 882–883.

[190] G. X. Jay Esfandyari, Roberto De Nuccio, “Introduction to MEMS gyroscopes,” *Solid State Technology*, 2010. [Online]. Available: http://electroiq.com/blog/2010/11/introduction-to-mems-gyroscopes/. [Accessed: 22-Jul-2016].

[191] D. Ren, L. Wu, M. Yan, M. Cui, Z. You, and M. Hu, “Design and analyses of a MEMS based resonant magnetometer,” *Sensors*, vol. 9, no. 9, pp. 6951–6966, 2009.

[192] “Technical Report, Hall Effect Sensor,” 2016. [Online]. Available: http://www.electronics-tutorials.ws/electromagnetism/hall-effect.html. [Accessed: 25-Jul-2016].

[193] X. Zhai *et al.*, “Application of ICmetrics for Embedded System Security,” in *2013 Fourth International Conference on Emerging Security Technologies*, 2013, pp. 89–92.

[194] J. Shao, X. Lin, S. Member, R. Lu, and C. Zuo, “Protocol for VANETs,” vol. 65, no. 3, pp. 1711–1720, 2016.

[195] E. Papoutsis, “Investigation Of The Potential Of Generating Encryption Keys For ICMetrics, PhD Thesis,” Kent University, 2009.

[196] N. B. Ergeneman O; Chatzipirpiridis G; Blom FB; Pokki J; Pané S; Del Toro MM;Sánchez JF; Sotiriou GA, “Oxygen sensing using microrobots,” in *Annual International Conference of the IEEE 2010 Aug 31*, 2010, pp. 1958–1961.

[197] “Technical report, Ultrasonic Ranging Module HC,” 2015. [Online]. Available: http://www.micropik.com/PDF/HCSR04.pdf. [Accessed: 15-Nov-2015].

[198] “MyAHRS Sensors manual users.” [Online]. Available: http://www.withrobot.com/myahrs_plus_en/.pdf. [Accessed: 20-Feb-2016].

[199] H. Tahir, R. Tahir, and K. McDonald-Maier, “Securing MEMS Based Sensor Nodes in the Internet of Things,” *2015 Sixth Int. Conf. Emerg. Secur. Technol.*, pp. 44–49, 2015.

[200] “Report, Mass Functions and Density Functions,” 2009.

[201] M. L. Dekking FM, Kraaikamp C, Lopuhaä HP, *Lecture Note, Discrete Random Variables, In A Modern Introduction to Probability and Statistics, Springer London.* pp. 41–55, 2005.

[202] R. H. Baayen, *Analyzing linguistic data: A practical introduction to statistics using R,*.

Language Arts & Disciplinesو Cambridge University Press., 2008.

[203] R. L. Wasserstein and N. A. Lazar, "The ASA's Statement on p -Values: Context, Process, and Purpose," *Am. Stat.*, vol. 70, no. 2, pp. 129–133, 2016.

[204] "Car 2 Car Communication Consortium, "The Handbook for Vehicle-to-X Cooperative Systems Simulation," 2011. [Online]. Available: https://www.car-2-car.org/index.php?id=forum2011. [Accessed: 27-Jul-2016].

[205] "TAPAS Cologne " Scenario." [Online]. Available: http://sumo.sourceforge.net/doc/current/docs/userdoc/Data/Scenarios/TAPASCologne.html,2011. [Accessed: 27-Jul-2016].

[206] V.Sorge/E.Ritter, "Autumn Semester 2015 Handout 6," Birmingham, 2015.

[207] T. R. B. Mihir, "Multi-property-preserving hash domain extension and the EMD transfor, International Conference on the Theory and Application of Cryptology and Information Security," pp. 299–314, 2012.

[208] "Manual interpretation of ns2 trace file." [Online]. Available: https://getch.wordpress.com/2010/11/20/manual-interpretation-of-ns2-trace-file/. [Accessed: 10-Oct-2016].

[209] "Official site for PropOverlap package." [Online]. Available: http://cran.r-project.org/web/packages/. [Accessed: 14-Oct-2015].

[210] J. J. Castillo Aguilar, J. A. Cabrera Carrillo, A. J. Guerra Fernández, and E. Carabias Acosta, "Robust Road Condition Detection System Using In-Vehicle Standard Sensors.," *Sensors (Basel).*, vol. 15, no. 12, pp. 32056–78, Jan. 2015.

[211] A. A. Eltahir and R. A. Saeed, "Performance Evaluation of an Enhanced Hybrid Wireless Mesh Protocol (E-HWMP) Protocol for VANET," pp. 95–100, 2015.

[212] A. A. Pouyan and M. Yadollahzadeh Tabari, "FPN-SAODV: using fuzzy petri nets for securing AODV routing protocol in mobile Ad hoc network," *Int. J. Commun. Syst.*, p. n/a-n/a, Feb. 2015.

[213] C. S. M. H. Aziz, Erik L. J. Bohez, "Classification of Fuzzy Petri nets, and their applications, World Academy of Science, Engineering and Technology 72 2010," pp. 586–593, 2010.

[214] T. Murata, "Petri Nets: Properties, Analysis and Applications," in *Proceedings of the IEEE*, 1989, vol. 77, no. 4.

[215] E. V. Balan, M. K. Priyan, C. Gokulnath, and G. U. Devi, "Fuzzy Based Intrusion Detection Systems in MANET," *Procedia Comput. Sci.*, vol. 50, pp. 109–114, 2015.

[216] S.-M. Shyi-Ming Chen, J.-S. Jyh-Sheng Ke, and J.-F. Jin-Fu Chang, "Knowledge representation using fuzzy Petri nets," *IEEE Trans. Knowl. Data Eng.*, vol. 2, no. 3, pp. 311–319, 1990.

[217] M. O. P. Albertos, A. Sala, "Fuzzy Logic Controllers. Methodology. Advantages and Drawbacks," pp. 833–844, 1998.

[218] R. I. Hamed, "Esophageal cancer prediction based on qualitative features using adaptive fuzzy reasoning method," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 27, no. 2, pp. 129–139, 2015.

[219] M. Gao, M. Zhou, and Y. Tang, "Intelligent decision making in disassembly process based on fuzzy reasoning petri nets.," *IEEE Trans. Syst. Man. Cybern. B. Cybern.*, vol. 34, no. 5, pp. 2029–34, 2004.

[220] R. I. Hamed, S. I. Ahson, and R. Parveen, "A new approach for modelling gene regulatory networks using fuzzy petri nets.," *J. Integr. Bioinform.*, vol. 7, no. 1, 2010.

[221] L. Wischhof, A. Ebner, and H. Rohling, "Information Dissemination in Self-Organizing Intervehicle Networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 6, no. 1, pp. 90–101, Mar. 2005.

[222] J. Sola and J. Sevilla, "Importance of input data normalization for the application of neural networks to complex industrial problems," *IEEE Trans. Nucl. Sci.*, vol. 44, no. 3 PART 3, pp. 1464–1468, 1997.

[223] M. Alreshoodi *et al.*, "Prediction of Perceptual Quality for Mobile Video Using Fuzzy Inference Systems," vol. 61, no. 4, pp. 546–554, 2015.

[224] Y. Peng, Z. Abichar, and J. Chang, "Roadside-Aided Routing (RAR) in Vehicular Networks," in *2006 IEEE International Conference on Communications*, 2006, vol. 8, pp. 3602–3607.

[225] E. M. van Eenennaam, W. Klein Wolterink, G. Karagiannis, and G. J. Heijenk, "Exploring the Solution Space of Beaconing in VANETs," 2009.

[226] C. Campolo, A. Vinel, A. Molinaro, and Y. Koucheryavy, "Modeling Broadcasting in IEEE 802.11p/WAVE Vehicular Networks, IEEE Communications Letters," vol. 15, no. 2, pp. 199–201, Feb. 2011.

[227] R. W. Supervisor and M. Scott, “Richard Whitehouse Implementation of Data Link Layer Protocols for a Network Simulator Implementation of Data Link Layer Protocols for a Network Simulator Original Aims of the Project,” 2011.

[228] H. Holma and A. Toskala, “WCDMA FOR UMTS, Radio Access for Third Generation Mobile Communications, Revised Edition. New York: Wiley, john Wiley & sons, 2001.”

[229] P. Djukic and P. Mohapatra, “Soft-TDMAC: A Software TDMA-Based MAC over Commodity 802.11 Hardware,” in *IEEE INFOCOM 2009 - The 28th Conference on Computer Communications*, 2009, pp. 1836–1844.

[230] U. Khan, S. Agrawal, and S. Silakari, “Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks,” *Procedia Comput. Sci.*, vol. 46, pp. 965–972, 2015.

[231] A. Karygiannis, E. Antonakakis, and A. Apostolopoulos, “Host-based network monitoring tools for MANETs,” in *Proceedings of the 3rd ACM international workshop on Performance evaluation of wireless ad hoc, sensor and ubiquitous networks - PE-WASUN ’06*, 2006, p. 153.

[232] Its, “EN 302 637-2 - V1.3.2 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service,” 2014.

[233] J. Grover, M. S. Gaur, and V. Laxmi, “A novel defense mechanism against sybil attacks in VANET, Proceedings of the 3rd international conference on Security of information and networks - SIN ’10,” pp. 249–255, 2010.

[234] ETSI (European Telecommunications Standards Institute), “ETSI TS 102 637-2 Vehicular Communications ; Basic Set of Applications ; Part 2 : Specification of Cooperative,” *History*, vol. 1, pp. 1–18, 2011.

[235] D. Y. Kim, J. M. Kim, H. Jang, J. Jeong, and J. W. Lee, “A neural network accelerator for mobile application processors,” *IEEE Trans. Consum. Electron.*, vol. 61, no. 4, pp. 555–563, Nov. 2015.

[236] W. Fan and P. S. Yu, “Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies,” pp. 1–25, 2002.

[237] T. Anantvalee and J. Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks, Wireless/Mobile Network Security Journal,” vol. 2, no. 5, pp. 170–196, 2006.

[238] F. Kargl *et al.*, "Topics in Automotive Networking Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges," vol. 46, no. 11, pp. 110–118, 2008.

[239] M. Al-Mutaz, L. Malott, and S. Chellappan, "Detecting Sybil attacks in vehicular networks," *J. Trust Manag.*, vol. 1, no. 1, p. 4, May 2014.

[240] P. Druschel, F. Kaashoek, and A. Rowstron, *Peer-to-peer systems : First International Workshop, IPTPS 2002, Cambridge, MA, USA, March 7-8, 2002 : revised papers*. Springer, 2002.

[241] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against Sybil attack in vehicular ad hoc network based on roadside unit support," in *MILCOM 2009 - 2009 IEEE Military Communications Conference*, 2009, pp. 1–7.

[242] R. C. Umar Faroog Minhas, Jie Zhang, Thomas Tran, "ijcitp.pdf," *Int. J. Comput. Intell. Theory Pract.*, vol. 5, no. 1, pp. 1–13.

[243] Qin Li, A. Malip, K. M. Martin, Siaw-Lynn Ng, and Jie Zhang, "A Reputation-Based Announcement Scheme for VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 9, pp. 4095–4108, Nov. 2012.

[244] S. Ruj, M. Antonio Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "Data-centric Misbehavior Detection in VANETs," 2011.

[245] A. Hern, "Car hacking is the future – and sooner or later you'll be hit, Published in The Guardian Newspaper." [Online]. Available: https://www.theguardian.com/technology/2016/aug/28/car-hacking-future-self-driving-security. [Accessed: 31-Jan-2017].

[246] "Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities." [Online]. Available: http://www.gartner.com/newsroom/id/2970017. [Accessed: 31-Jan-2017].

[247] K. S. and X. S. Redouane Khemmar, Jean-Yves Ertaud, "V2G-based Smart Autonomous Vehicle For Urban Mobility using Renewable Energy," in *The Fourth International Conference on Smart Systems, Devices and Technologies*, 2015, pp. 62–68.

[248] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks," in *Ad Hoc Networks*, 2003, vol. 1, no. 1, pp. 175–

192.

[249] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,” in *in Proc. Eighth ACM International Conference on Mobile Computing and Networking*, 2002, pp. 21–38.

[250] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, “A Secure Routing Protocol for Ad Hoc Networks,” in *Icnp*, 2002, pp. 78–89.

[251] S. Yi, P. Naldurg, and R. Kravets, “Security-aware ad hoc routing for wireless networks,” in *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing - MobiHoc ’01*, 2001, p. 299.

[252] J. Martin, L. Manickam, R. Bhuvaneswari, M. A. Bhagyaveni, and S. Shanmugavel, “Secure Routing Protocol for Mobile Ad-Hoc Networks,” in *in Proc. Summer Computer Simulation Conference*, 2007, pp. 725–731.

[253] P. Papadimitratos and Z. J. Haas, “Secure link state routing for mobile ad hoc networks,” in *2003 Symposium on Applications and the Internet Workshops, 2003. Proceedings.*, 2003, pp. 379–383.

[254] M. G. Zapata, “Secure Ad hoc On-Demand Distance Vector Routing,” *ACM Mob. Comput. Commun. Rev.*, vol. 6, no. 3, pp. 106–107, 2002.

[255] B. Lu and U. W. Pooch, “Cooperative security-enforcement routing in mobile ad hoc networks,” in *4th International Workshop on Mobile and Wireless Communications Network*, 2002, pp. 157–161.